Grenze International Journal of Engineering and Technology, June Issue

Data Encryption Strategy in Cloud Computing with Malware Detection

S .Giridharan[1], B. Aravinthan[2], SA. Hajitha Shree[3] and R. Harish Kumar[4]
[1]Assistant professor[1], Department of Cybersecurity, SRM Valliammai Engineering College
Email: giri@gmail.com
[2-4]UG scholar, Department of Cybersecurity, SRM Valliammai Engineering College
Email: alluaravind87@gmail.com, hajitha098@gmail.com, harish12groot@gmail.com

***Abstract*— Mobile cloud computing provides network operators, cloud providers, and mobile users with vast computational resources by fusing mobile computing, cloud technologies, and wireless networks. Complex mobile apps may now function across several devices, with data processing and storage taking place off of mobile devices. Mobile cloud computing has become commonplace with the growth of large data and mobile devices. The cloud facilitates data management by processing and storing data. Data categorization, segmentation, encryption technique selection, key management, and safe data transit and storage are just a few of the modules that must be integrated into a privacy-centric data encryption strategy for big data in mobile cloud computing. Strategies like AES, FERNET, and RES have been modified to meet the demands of large data. These methods employ SQLite or metadata to store documents and create a hybrid cloud for users. Users have a time constraint on how long they have to supply an operational key in order to access files that require email OTP verification. In the age of mobile cloud computing, sensitive data may be protected with a strong privacy-centric data encryption approach by integrating these modules in an efficient manner.**

***Index Terms*— Privacy-centric, Data encryption, Cloud computing, Email-otp.**

I. INTRODUCTION

The enormous volumes of data being created and utilized in today's data-driven society make protecting sensitive information essential. Privacy is seriously threatened by the convergence of cloud computing. We provide a privacy-centric data encryption strategy designed especially for big data in mobile cloud computing settings to address this problem. In order to ensure data security, a strong privacy-focused data encryption policy is necessary. By respecting individual privacy rights, this approach tackles data security at rest, in transit, and during processing. Calculations on encrypted data are possible using homomorphic encryption, which conceals the contents of the data. The computing power of homomorphic encryption varies depending on its nature. Encrypted data must be stored securely and a secure homomorphic encryption scheme must be used. In conclusion, a thorough Privacy-Centric Data Encryption plan is required to safeguard sensitive data in the era of Big Data and Mobile Cloud Computing. This strategy seeks to preserve individual privacy rights, safeguard data, and provide effective data analysis.

II. RELATED WORK

[1].Cloud-based data analytics and artificial intelligence are used by the CLARIFY project, which is supported by

Grenze ID: 01.GIJET.10.2.198

the Marie Sklodowska-Curie Actions programme of the European Union, to create a dependable digital diagnosis platform. Specifically, we use smart contract-based access control and decentralized identity technology at the system security boundary to ensure the flexibility and immutability of verification. To put privacy, computational efficiency, and usability first, technologies including blockchain, federated learning, dataset distillation, and differential privacy are used. Improved usability and privacy-preserving computer technologies are the goals of the project.

[2].This paper examines the security vulnerabilities associated with 5G-enabled wireless access networks for social robots in public places. It takes into account risks to user devices, ad hoc network connectivity, and SR and access points. Various dangers are identified by the study, including side-channel, physical, injection, manipulation, intrusion, injection, malevolent, and natural hazards. Post-quantum cryptography and early physical security implementation in architecture are among the recommendations.The findings confirm that the RAN of SRPS is most vulnerable to physical, side-channel, intrusion, injection, manipulation, and natural and malicious threats.

[3].An in-depth analysis of federated learning (FL) in artificial intelligence (AI) emphasises cooperative model training while maintaining user privacy. Identify trustworthiness pillars and evaluation metrics specific to FL models, as well as to develop solutions for computing trustworthiness levels. It describes the four cornerstones of reliable FL: fairness, security, privacy, and interpretability. The survey assesses trust assessment instruments and suggests a thorough architecture for reliable FL. By using this resource, AI systems may be made safer and more dependable.

[4].This dissertation employs quantitative, qualitative, and systematic literature review methodologies to investigate internet censoring strategies and processes. A reference model for internet restriction technologies is suggested, and several censorship strategies and technological hazards are discussed. It demonstrates worldwide trends in internet filtering by using data from 70 nations analyzed, 62 used at least one Internet censorship method against their citizens. The results reveal worldwide trends in Internet censorship based on historical evidence and Internet measurement data.

[5].Since the 2019 INTERPOL International Forensic Sciences Management Symposium, there have been breakthroughs in forensic handwriting and document examination. This paper evaluates these developments. In question document forensic labs, it seeks to improve technology capabilities and execution. The review covers significant topics such as trends, problems, gaps in the area, quality assurance, and forensic intelligence. Although pointing out certain omissions, the writers accept the scientific basis for publications and talks.

III. Architectural Diagram

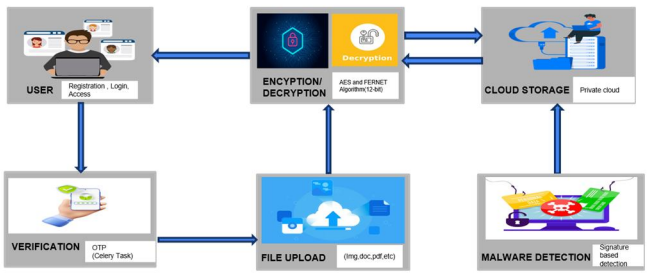

Figure 1 (Proposed Architectural Diagram)

IV. Proposed Work

A. ENCRYPTION ALGORITHM SELECTION

In the encryption algorithm to guarantee good security and compatibility, a number of things must be taken into account. The algorithm's performance, cryptographic strength, and fit for a given task must all be balanced. The robustness of AES, RSA, and ECC is well known, and they pass tests against NIST and FIPS standards. It's crucial to evaluate elements like assault resistance and key length. Performance is important, particularly in settings with limited resources when some algorithms (like AES) put speed ahead of security. It is essential to keep abreast of algorithmic developments and weaknesses in order to future-proof security protocols. To guarantee data security and integrity, the selection procedure often entails assessing encryption strength, performance, compliance, and flexibility. Updating frequently is required to stay on top of changing risks and requirements.

B. USER REGISTRATION

User registration is an important stage in web applications since it allows users to create accounts and access personalised features securely. To guarantee user-friendliness, data security, and authentication, this procedure entails several steps. Through a registration form, users provide vital information including their username, email address, and password. The form is then validated to ensure accuracy and completeness. Platform security is improved by additional authentication methods like CAPTCHA or email verification, which stop automated bot registrations. Following a successful registration, user data is safely kept in databases in accordance with data protection laws like the GDPR. Features like profile customisation for information management and preference management are frequently included when registering a user. By lowering friction during onboarding, a shortened registration process improves user engagement and retention.

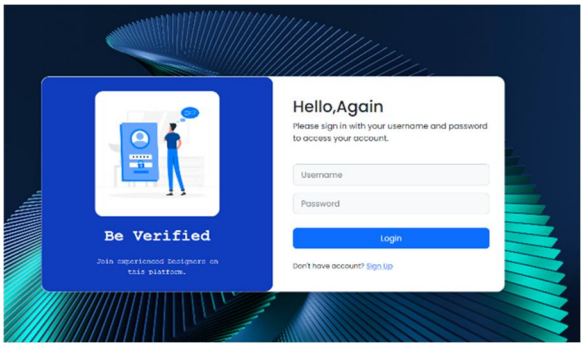

Figure 2 (User Register Page)

C. USER AUTHENTICATION

User authentication verifies the identity of people who use digital platforms or services, enabling only authorised users access. Users enter usernames and passwords, which are then encrypted and hashed in a database. Additional security layers, such as two-factor authentication (2FA) or multi-factor authentication (MFA), necessitate additional verification in the form of one-time passwords (OTP), biometric data, or hardware tokens. Session management keeps users locked in during sessions, while SSL/TLS secures communication. Rate limiting, CAPTCHA difficulties, and account lockout restrictions are all examples of attack defences. Balancing security and ease is critical for a seamless experience. User authentication safeguards systems and data against breaches by establishing trust through strong verification mechanisms and encryption.

Figure 3 (OTP VERIFICATION)

D. FILE SECURE STORAGE

Implementing a secure file storage system necessitates a comprehensive approach that includes encryption, access control, secure transmission, data accuracy, audit logging, recovery and backup, physical security, compliance, reliable development practices, training users, monitoring, as well as patch administration. Encryption is the foundation, guaranteeing that files stay inaccessible to unauthorised entities. Encrypting files with robust methods like AES protects their information. Access control techniques are then implemented to limit file access to just authorised users, commonly using authentication and authorization protocols such as role-based access control.

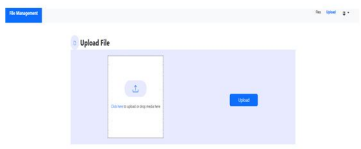

Figure 1.4 (File Upload Page)

E. MALWARE DETECTION

Malware detection necessitates a holistic approach that integrates numerous approaches and technologies in order to successfully identify and combat malicious software threats. The foundation is built on powerful anti-virus and anti-malware software that uses signature-based scanning to detect known malware strains and behaviours, as well as real-time monitoring capabilities for quick threat neutralisation. Beyond typical detection methods, heuristic analysis tools examine file properties, code structures, and behavioural patterns to identify potential risks. Behavioural analysis strengthens defences by monitoring software operations for suspect activity, such as unauthorised file alterations or network communications. Through advanced algorithms, these systems continuously develop their ability to detect and classify potential risks based on file attributes and system behaviours.

F. CLOUD DEPLOYMENT

Implementing cloud deployment on Vercel requires a streamlined procedure that takes advantage of its serverless architecture and simple deployment workflows. First, design your file storage system by defining components such as front-end interfaces, back-end services, databases, and authentication techniques. Create the system using appropriate technologies and frameworks. Monitor the deployed application's performance and security by using logging and monitoring tools to track usage and spot irregularities. Regularly update and maintain the system in order to resolve vulnerabilities and introduce new features. Following these steps will allow you to successfully establish a secure file storage system on Vercel, leveraging its scalability, dependability, and user-centric deployment processes to offer a robust solution.

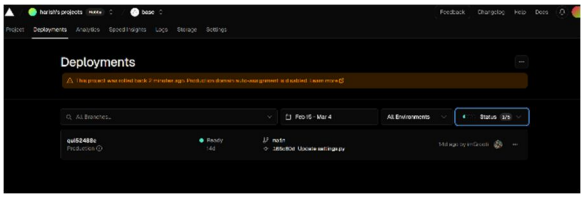

Figure 5 (Cloud Deployment Dashboard)

V. CONCLUSION

In an era where data breaches and privacy violations are constant dangers, this method serves as a safeguard against potential weaknesses, ensuring that organisations and people' sensitive information stays discreet and secure. By meticulously addressing encryption technologies, key management, and usability preservation, this strategy establishes a healthy balance between data safety and operational efficiency. Implementing a Data Encryption Strategy with Malware Detection is not an option; it is required for protecting the integrity and trustworthiness of our digital environment.

REFERENCE

[1] Geng. J, Mou. Y, Li, Q., Li, F., Beyan, O., Decker, S., Rong, C. “Taking Computation to Data: Integrating Privacy-preserving AI techniques and Blockchain Allowing Secure Analysis of Sensitive Data on Premise”, 2023.

[2] Samson, oruma.S, & petrovic,S. “Security threats to 5G networks for social robots in public spaces:A Survey”. In IEEE Access, 2023.

[3] Tariq, A.,Serhani,M.A.,Sallabi,F.,Qayyum,T.,Barka,E.S.,&Shuaib,K.A.,“Trustworthy federated learning: A Survey. arXiv preprint”, 2023.

[4] Master.A. “Modeling and Characterization of Internet Censorship Technologies”. CERIAS Tech Report, 2023.

[5] Paul Reedy.P, “Interpol review of digital evidence for 2019–2022”,Forensic Science International: Synergy, 2023.

[6] Peladarinos. N., Piromalis, D., Cheimaras, V., Tserepas, E., Munteanu, R. A., &Papageorgas, P. “Enhancing Smart Agriculture by Implementing Digital Twins: A Comprehensive Review. Sensors”, 2023.

[7] Al khodair, A. J., Mohanty, S. P., & Kougianos, E. FlexiChain 2.0: “NodeChain Assisting Integrated Decentralized Vault for Effective Data Authentication and Device Integrity in Complex Cyber-Physical Systems”,(2023).

[8] Gharavi, H. “Post Quantum Blockchain Security for the Internet of Things Survey and Research Directions”,(2023).

[9] Rawat, Danda B., “Ronald Doku, and Moses Garuba. “Cybersecurity in the big data era: From securing big data to data-driven security”, IEEE Transactions on Services Computing,(2023).

[10] Sasikumar, A., Logesh Ravi, Ketan Kotecha, Ajith Abraham, Malathi Devarajan, and Subramaniyaswamy Vairavasundaram. “A Secure Big Data Storage Framework based on Blockchain Consensus Mechanism with Flexible Finality”, IEEE Access (2023)