International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

DESIGNING CLOAKING WALL MODEL WITH LEAKAGE- SUPPRESSED AND LIGHTWEIGHT ACCESS CONTROL FOR CLOUD DATA STORAGE

Mr. Rajasekar L
Electronics and communication Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India
rajasekar.ec20@bitsathy.ac.in

Mr. Srinivasan S
Electronics and communication Engineering
Bannari Amman Institute Of technology
Sathyamangalan,India
srinivasan.ec20@bitsathy.ac.in

Abstract— **In the era of cloud computing, ensuring the security and privacy of sensitive data has become paramount. The aim of this project is to develop a cutting-edge model to fortify cloud data storage systems against unauthorized access and information leakage. The Cloaking Wall Model addresses the challenge of data leakage through the implementation of state-of-the-art leakage suppression techniques. Leveraging advanced cryptographic protocols and anomaly detection algorithms, the model intelligently identifies and mitigates potential data leakage threats, safeguarding sensitive information from unauthorized disclosure. The Cloaking Wall Model enhances cloud data security through Long-Term, Multi-Region, Time-based, and Geolocation-based cloaking methods. By integrating these features, the system addresses vulnerabilities associated with data leakage and ensures efficient access control. The model introduces a lightweight access control mechanism, aiming to strike a balance between robust security and operational efficiency. Traditional access control methods often introduce significant computational overhead, impacting the overall performance of cloud systems. In contrast, the lightweight access control in the Cloaking Wall Model optimizes resource utilization, ensuring rapid and secure data access without compromising system efficiency. The cryptographic protocols employed in leakage suppression not only encrypt and obfuscate data but also generate encrypted keys that are verified during the access control process. This ensures the integrity and authenticity of the data, preventing the unauthorized alterations. The Cloaking Wall model contributes to advancing secure cloud storage paradigms by providing a comprehensive solution that balances robust security in the cloud environment.**

Keywords— Long term cloaking, Multi-Region cloaking, Time and Geolocation cloaking, Chacha20.

I. Introduction

In the age of digital transformation, cloud storage solutions are being used by businesses of all sizes because they offer unmatched scalability, flexibility, and affordability for handling enormous amounts of data. Without requiring substantial on-premises infrastructure, enterprises may safely store enormous volumes of data by utilizing remote servers hosted on the internet. Cloud storage makes information easily accessible at any time and from any location, which promotes productivity and teamwork. From small startups to multinational corporations, industries spanning diverse sectors such as finance, healthcare, education, and entertainment are embracing the cloud as a central component of their digital infrastructure. The rapid growth can make data generation and the ever-expanding demands for storage capacity, the adoption of cloud storage solutions continues to soar, revolutionizing the way businesses manage and utilize their data assets. In the fast-paced world of IT industries, cloud storage solutions like Google Drive, Microsoft OneDrive, and similar platforms play a pivotal role in data management, collaboration, and productivity enhancement. These cloud storage platforms serve as repositories for storing vast amounts of data securely. IT professionals utilize them to store various types of files, including documents, presentations, spreadsheets, code repositories, and multimedia files. Cloud storage eliminates the need for on-premises infrastructure, reducing costs and providing scalability to accommodate growing data volumes. These platforms offer seamless collaboration features. In the ever-expanding landscape of cloud data storage, ensuring the security and confidentiality of sensitive information is paramount. Traditional encryption methods have long been relied upon safeguarding data from unauthorized users, however the leakage of data is serious issue. Cloud leakage, in simple terms, refers to the unintended or unauthorized disclosure of sensitive information stored in cloud computing systems. Just like a leak in a water pipe can result in water escaping where it should not, cloud leakage involves data escaping from where it is supposed to be securely stored. This can occur due to various factors, including human error, misconfigurations, cyberattacks, or inadequate security measures. Lightweight access control mechanisms are essential to ensure efficient management of access permissions without imposing significant computational overhead. As the project aims to develop a cloaking wall model for cloud data storage, lightweight access control will help minimize performance impact and resource utilization, enabling seamless integration with existing cloud infrastructure. With the increasing volume and complexity of data stored in cloud environments, scalability is crucial. Lightweight access control mechanisms are necessary to support large-scale cloud deployments and accommodate growing numbers of users, files, and access requests. They enable organizations to effectively manage access permissions across distributed cloud environments without sacrificing performance or scalability. This innovative approach seeks to address the shortcomings of existing encryption techniques while minimizing the computational overhead typically associated with stringent security measures. By leveraging advanced algorithms and emerging technologies, the envisioned cloaking wall model will provide a robust defense against unauthorized access and data breaches.

Literature Survey

Shota Fuji et.al.[1] in their paper discussed about malicious hosts and their behavior. Malicious hosts are services that allows hackers to rent software and hardware for conducting cyber-attacks. The proposed research work explains about long term cloaking, multiregional cloaking, and geolocation-based cloaking. The objective of this paper is to find the longevity of malicious hosts employing cloaking and their ability to evade existing detection technologies. They proposed Stargazer as a monitoring system for malicious hosts, to collect data over an extended period. It can detect both geofencing and time-based cloaking. The research concluded that malicious hosts are threat to cloud data storage. Effective encryption algorithms need to be used to safeguard the cloud data from malicious attacks. Arun Kumar Sangaiah et.al.[2] in their paper focused on cloud data storage techniques. To emphasize the significance of guaranteeing data availability, confidentiality, and integrity in cloud environments, the study starts off by going over the basic ideas and difficulties of cloud data storage security. It explores the several risks and weaknesses that cloud storage systems must deal with, such as illegal access, data breaches, and data leaks. The authors reviewed the literature on access control methods for cloud storage, including attribute-based access control, role-based access control, and fine-grained access control. It also explains the deduplication techniques in cloud storage, which aim to eliminate redundant data to conserve storage space and improve efficiency. The authors surveyed different deduplication algorithms and methodologies and discussed their impact on data security. Shangping Wang et.al. [3 in their paper discussed about the limitations of Attribute Based Encryption for fine-grained access control and data privacy in traditional cloud storage systems. It highlights limitations related to scalability, centralized trust models, and potential single points of failure. In Attribute based encryption to reduce the corresponding costs the cipher text for the scheme should be as short as possible. They also suggested to use symmetric encryption algorithm so that the computation load can be reduced. Their proposed framework can be directly used by combining with symmetric searchable encryption algorithms. However, the research did not explain data user point of view, Ishu Gupta, Ashutosh Kumar Singh [4in their paper have researched cloud computing automated security analysis and enforcement using graphical security models. Cloud Safe, an automated cloud security assessment tool is described by the author in this publication. The study uses a methodology that combines vulnerability patching, virtual patching, network hardening, and moving target defence. The proposed system detects the malicious users by combination of probability estimation and watermark extraction. Documents of various sizes are fed to the model to evaluate the model's efficiency. The proposed work takes less computational time. However this research does not explain anything about the light weight access control. Sajid Habib Gill et.al. [5] in their paper explained about the acceleration of cloud computing with grid computing, distributed computing, and utility computing. The research provides a detailed analysis on security and privacy challenges in the cloud. The leading cloud service providers are Rackspace, Amazon, Microsoft, and Google. Three different types of services are offered by the cloud. Cloud service models like platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS) can be used to access data on the cloud. [6] addressed the challenges and proposed solutions for aligning eIDAS regulations with self-sovereign identity systems. Their work emphasizes the importance of regulatory compliance and interoperability in fostering the adoption of SSI frameworks. Additionally, Gajraj Kuldeep et.al. [7] evaluated and discussed the Multi-class Privacy-Preserving Cloud Computing (MPCC) program, which protects multilevel data privacy in Internet of Things applications. The MPCC approach performs computationally intensive sparse signal recovery in a privacy-preserving way by using compressive sensing. The compressive sensing (CS), a crucial method for recovering sparse and compressible signals, is the algorithm used. The work explains about the reduced computational complexity at IoT sensor devices and data end-users. Bonthala Prabhanjan Yadav and Ch. Shiva Sai Prasad, [8] have researched cloud computing's use of biometric authentication. The paper's goal is to successfully safeguard cloud computing users' privacy when using biometric authentication. The methodology used here is encrypting the biometric information before transferring it to the Cloud database during a biometric verification. This paper focuses on encryption procedure and cloud verification guarantee to protect the confidentiality of biometric data during the authentication process. Hongbo Li et.al. [9] explored identity-based ciphertexts' permitted equality test for sharing confidential data via cloud storage. In this work, the authors employed a method called IBEET-FA based bilinear pairing to determine whether the two ciphertexts are encrypted using distinct keys. Cryptographic protocols use the computational approach of bilinear pairing, and IBEET-FA facilitates the equality test of ciphertexts encrypted with various keys. Wenting Shen et.al. [10] proposed a deduplication-supported cloud storage auditing technique that provides robust privacy protection, ensuring that user privacy is maintained when storing files in a minimal or predictable amount of space and not shared with the cloud or other parties. Convergent encryption (CE) encrypts data using a message-dependent key to facilitate deduplication over encrypted data.

II. SOFTWARE SPECIFICATIONS

A. Python 3.7.4:

Python is a versatile programming language known for its simplicity, readability, and vast ecosystem of libraries and frameworks. Python's extensive ecosystem of libraries and frameworks provides robust solutions for implementing key components of the project. Python allows developers to design and implement the cloaking wall model's core functionality, including data obfuscation, encryption, and access control mechanisms. Python frameworks like Flask or Django can be employed to create a user-friendly interface for interacting with the cloaking wall model and managing access controls.

B. MySQL:

MySQL is an open-source relational database management system (RDBMS) which involves tables. MySQL serves as the backend database to store essential information such as user credentials, access control policies, audit logs, and metadata related to the cloaking wall model.

C. *WampServer:*

WampServer, Configured to host the Flask application locally, providing a development environment for testing and debugging. This helps improve the accessibility and usability of the application, enhancing the user experience for data owners, administrators, and end-users interacting with the cloaking wall model and associated features.

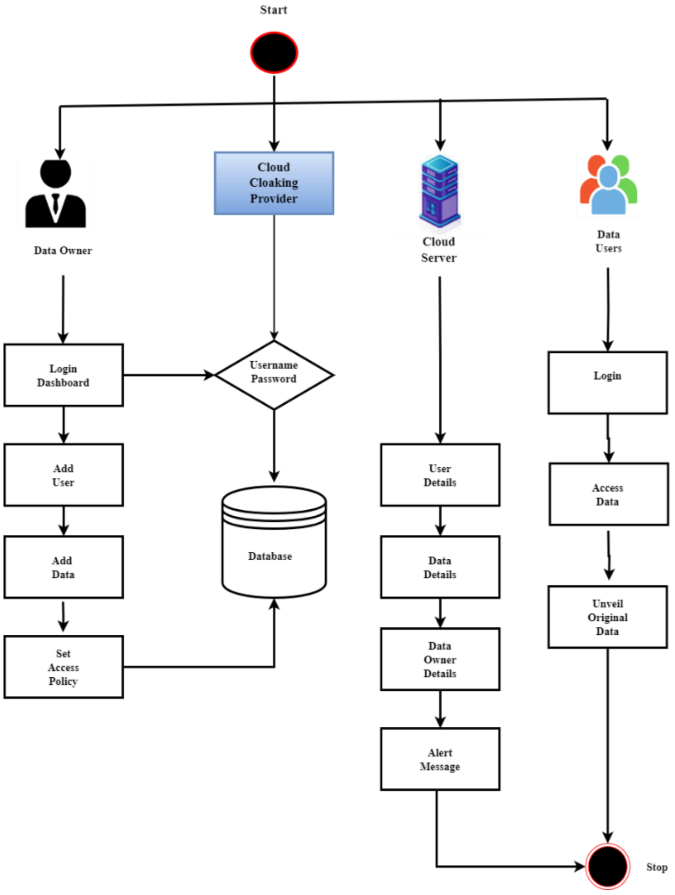
D. Flask:

Flask can be employed to develop the backend server-side components, including the API endpoints and business logic of the cloaking wall model. With Flask, developers can quickly create RESTful APIs to handle data retrieval, manipulation, and authentication. Flask's simplicity and modularity allow for easy integration with other Python libraries and frameworks, making it suitable for implementing complex functionalities required by the cloaking wall model.

E. Bootstrap4:

Bootstrap is a popular front-end framework for building responsive and mobile-first web applications. By using Bootstrap, developers can leverage its responsive design features to ensure that the user interface adapts seamlessly to various devices, including desktops, tablets, and smartphones. This helps improve the accessibility and usability of the application, enhancing the user experience for data owners, administrators

III. FLOW CHART



IV. PROPOSED WORK

The system flow of the Cloaking Wall Model encapsulates a seamless and secure journey for users as they interact with the platform. Below is a detailed overview of the key steps and interactions within the system:

1. Development of Cloud Web App:

Developing a cloud web application involves several steps to ensure the creation of a robust, scalable, and secure application tailored specifically for cloud data storage environments. Requirement gathering and analysis involves defining the requirements and objectives of the cloud web application. Identifying the functionality, features, and user interactions required to implement the cloaking wall model, leakage suppression mechanisms, and lightweight access control plays a crucial role in development of cloud web application.

2. Development of User Interface:

The user interface (UI) plays a crucial role in facilitating user interactions with the cloud web application. The UI is designed in such a way that is intuitive and user-friendly, allowing users to easily navigate the application and access its features. Clear navigation menus, logical information architecture, and intuitive controls contribute to a positive user experience. The UI design is visually appealing, incorporating appropriate colors, typography, icons, and imagery. A cohesive design language and consistent visual elements helps to create a professional and polished appearance for the application.

3. Development of Cloaking Wall Model:

Development of cloaking wall model involves creating a robust and effective mechanism to protect sensitive data stored in the cloud from unauthorized access and data leakage. Development of dynamic data masking capabilities to selectively reveal or conceal sensitive data based on the user's access permissions ensures that only authorized users can view the sensitive information while others see masked or obfuscated data. Fine-grained access control mechanisms Integration into the cloaking wall regulates access to different data elements or attributes based on user roles, permissions, or data sensitivity levels.

4. Long Term Cloaking:

This method focuses on providing extended protection for sensitive data over prolonged durations. It involves concealing access patterns and data usage trends over an extended timeframe, ensuring persistent confidentiality. Long-term cloaking contributes to maintaining the privacy and security of stored data over extended periods, preventing unauthorized inference from patterns of access.

5. Multi Region Based Cloaking:

Recognizing the global nature of cloud services, multi-region-based cloaking involves implementing security measures that transcend geographical boundaries. By considering the diverse locations from which data access may occur, this method ensures a consistent and standardized security posture globally. It addresses the challenges associated with data access from different regions, providing a unified approach to access control policies.

6. Time Based Cloaking:

Time-based cloaking introduces temporal restrictions on data access, allowing organizations to define specific time windows during which data can be accessed. This method enhances security by limiting access to predefined timeframes, reducing the exposure of data to potential threats. Time-based cloaking adds an additional layer of control to access patterns, contributing to a more secure cloud data storage environment.

7. Geolocation-based cloaking:

Geolocation-based cloaking involves tailoring data protection measures based on the geographical location of users. This method adds a location-sensitive layer of security, ensuring that access to sensitive data is contingent on the user's physical location. Geolocation-based cloaking is particularly relevant for organizations with diverse and dispersed user bases, providing a customized approach to access control based on geographic parameters.

8. Chaffing and Winnowing:

Chaffing and Winnowing is a cryptographic algorithm that enhances the security and privacy of transmitted data by introducing decoy information and subsequently isolating the genuine content. Chaffing and Winnowing provide a mechanism to obfuscate data during transmission by blending genuine information with decoy elements and then selectively extracting the real content using a secure key or algorithm. This technique contributes to the confidentiality and integrity of transmitted data, particularly in scenarios where privacy and protection against unauthorized interception are paramount.

9. ChaCha20:

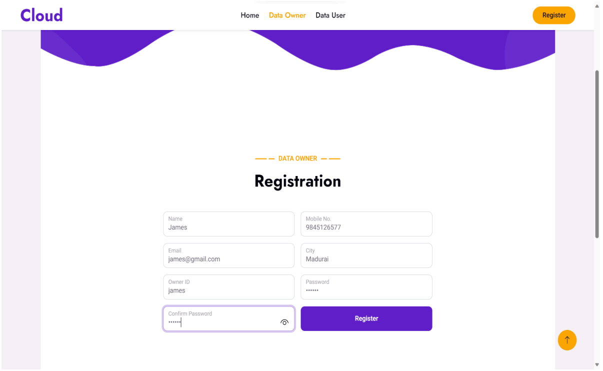
ChaCha20 is a contemporary encryption technique that uses a symmetric key stream cipher. This stream cipher, which is a member of the Salsa20 family, was created by Daniel J. Bernstein. ChaCha20 is renowned for its cryptanalysis-resistant design, speed, and simplicity. The goal of the ChaCha20 encryption algorithm is to offer both speed and security. It is built to withstand well-known attacks, such as linear and differential cryptanalysis. Furthermore, because of its great parallelizability, multi-core CPUs and other high-performance computing systems may readily be used with it. As a stream cipher, ChaCha20 encrypts data continuously as opposed to in fixed-size blocks. The ciphertext is created by XORing the pseudo-random bits in the continuous keystream that is generated with the plaintext data.

10. Firewalls and Network Security:

Firewall and network security measures are essential components for protecting the infrastructure, communication channels, and data stored in the cloud. Incoming and outgoing network traffic is watched over and managed by firewalls using pre-established security rules. This lessens the possibility of cyberattacks and unwanted access.

V. Result

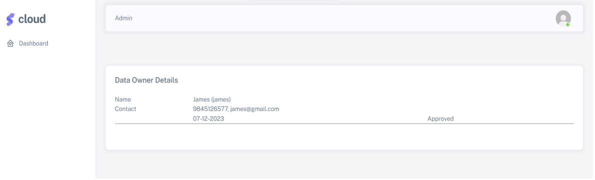
The cloaking wall model results in protecting the data leak in the cloud and ensures the robustness of data. The user-friendly environment helps to interact with the web application where the light weight access control can be managed and maintained for the users.



DATA OWNER

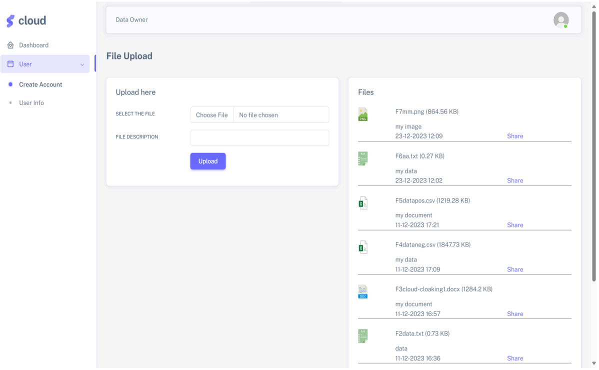
Registration

Name James	Mobile No. 9845126577
Email james@gmail.com	City Madurai
Owner ID james	Password ••••••
Confirm Password ••••••	Register



Data Owner Details

Name James (james)
Contact 9845126577, james@gmail.com
07-12-2023 Approved



File Upload

Upload here

SELECT THE FILE: No file chosen

FILE DESCRIPTION:

Files

F7mm.png (864.56 KB)
my image
23-12-2023 12:09

F6aa.txt (0.27 KB)
my data
23-12-2023 12:02

F5datapos.csv (1219.28 KB)
my document
11-12-2023 17:21

F4dataneg.csv (1847.73 KB)
my data
11-12-2023 17:09

F3cloud-cloaking1.docx (1284.2 KB)
my document
11-12-2023 16:57

F2data.txt (0.73 KB)
data
11-12-2023 16:36

The project focuses on advancing cloud data security through the implementation of a comprehensive Cloaking Wall Model integrated with advanced camouflage techniques within a Cloud Consumer Web App. This web application consists of various interconnected modules designed to streamline cloud resource management while ensuring robust security measures. The user authentication module serves as a secure entry point, employing multi-factor authentication for enhanced security. The dashboard module, at the core of the application, provides an intuitive interface for users to manage cloud resources comprehensively. Integrated with the Cloaking Wall Model, this module ensures global consistency in security measures. The End User Interface comprises distinct modules for Admins or Data Owners and Data Users. Admins can securely log in, add/manage data, users, provide login credentials, set access policies using the Cloaking Wall Model, and monitor data access. Data Users, on the other hand, access allocated data and monitor their own data access. The Cloaking Wall Model itself consists of Long-Term Cloaking, Multi-Region based Cloaking, Time-Based Cloaking, and Geolocation-Based Cloaking modules, providing advanced data protection and access control. The Access Policy Configurator empowers administrators to define and customize access policies based on these principles. The Bot Identification and Data Distribution module ensures the identification of automated bots and selectively distributes content based on policy adherence. The Disguise Data Generator Employs Chaffing and Winnowing with ChaCha20 encryption, generating malicious data for non-compliant users. Monitoring and Auditing capture real-time activities, and the Alerts and Notification module provides immediate alerts for policy violations.

VI. Applications

The project aims to ensures data confidentiality at rest, in transit, and during processing. Provides a standardized security posture globally. Distinguishes between authorized and unauthorized user for targeted content distribution. Reduces administrative workloads through efficient certificate management. Provides an advanced layer of data privacy, ensuring that sensitive information remains confidential during transmission. Minimizes the risk of unauthorized access. A crucial aspect highlighted is the ability to distinguish between authorized and unauthorized users for targeted content distribution. This feature enables organizations to control access to sensitive information, ensuring that only those with the appropriate permissions can view or interact with specific data sets. Efficient certificate management is also emphasized as a means of reducing administrative workloads. By automating the issuance, renewal, and revocation of security certificates, the solution streamlines the process and minimizes the risk of human error, thus enhancing overall security posture.

VII. Consclusion

In conclusion, the initiative presents a solid way to improve cloud computing data security. Persistent secrecy and worldwide consistency are guaranteed by the Cloaking Wall Model, which includes features like Geolocation-based Cloaking and Long-Term Cloaking. The Camouflage Data Disguise technique, integrating Chaffing and Winnowing with ChaCha20 encryption, adds an extra layer of defense. The Cloud Consumer Web App's modular design caters to both administrators and users, offering secure functionalities like user authentication, data management, and monitoring. The project's testing phase, outlined in the test report, demonstrates a rigorous approach to quality assurance. The innovative Bot Identification Mechanism, coupled with the Disguise Data Generator module, adds an intelligent layer to the security framework. By accurately identifying potential bot activity and simulating non-compliant data instances, the system actively responds to emerging threats. The Monitoring and Auditing modules, along with the immediate Alerts and Notifications system, empower administrators to maintain real-time oversight, respond promptly to policy violations, and uphold the integrity of the system. Thus, the project provides a adaptive solution to evolving cloud data security challenges, aligning with the demands for secure and privacy-preserving cloud computing practices.

VIII. References

1] S. Qi, W. Wei, J. Wang, S. Sun, L. Rutkowski, T. Huang, et al., "Secure data deduplication with dynamic access control for mobile cloud storage", IEEE Trans. Mobile Comput., pp. 1-18, 2023.

2] Y. Chen, J. Li, C. Liu, J. Han, Y. Zhang and P. Yi, "Efficient attribute based server-aided verification signature", IEEE Trans. Services Comput., vol. 15, no. 6, pp. 3224-3232, Nov. 2022.

3] P. Patil and M. Sangeetha, "Blockchain-based decentralized KYC verification framework for banks", Proc. Comput. Sci., vol. 215, pp. 529-536, Jan. 2022.

4] X. Li, T. Liu, C. Chen, Q. Cheng, X. Zhang and N. Kumar, "A lightweight and verifiable access control scheme with constant size ciphertext in edge-computing-assisted IoT", IEEE Internet Things J., vol. 9, no. 19, pp. 19227-19237, Oct. 2022.

5] P. Sanchol, S. Fugkeaw and H. Sato, "A mobile cloud-based access control with efficiently outsourced decryption", Proc. 10th IEEE Int. Conf. Mobile Cloud Comput. Services Eng. (MobileCloud), pp. 1-8, Aug. 2022.

6] S. Fugkeaw, "A lightweight policy update scheme for outsourced personal health records sharing", IEEE Access, vol. 9, pp. 54862-54871, 2021.

7] J. Sun, D. Chen, N. Zhang, G. Xu, M. Tang, X. Nie, et al., "A privacy-aware and traceable fine-grained data delivery system in cloud-assisted healthcare IIoT", IEEE Internet Things J., vol. 8, no. 12, pp. 10034-10046, Jun. 2021.

8] J. Gao, H. Yu, X. Zhu and X. Li, "Blockchain-based digital rights management scheme via multiauthority ciphertext-policy attribute-based encryption and proxy re-encryption", IEEE Syst. J., vol. 15, no. 4, pp. 5233-5244, Dec. 2021.

9] Y. Lin, J. Li, X. Jia and K. Ren, "Multiple-replica integrity auditing schemes for cloud data storage", Concurrency Comput. Pract. Exper., vol. 33, no. 7, pp. 1, Apr. 2021.

10] S. Wang, H. Wang, J. Li, H. Wang, J. Chaudhry, M. Alazab, et al., "A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare network", IEEE Trans. Ind. Appl., vol. 56, no. 4, pp. 4467-4477, Jul. 2020.

11] Z. Li, W. Li, Z. Jin, H. Zhang and Q. Wen, "An efficient ABE scheme with verifiable outsourced encryption and decryption", IEEE Access, vol. 7, pp. 29023-29037, 2019.

12] Q. Li, Y. Tian, Y. Zhang, L. Shen and J. Guo, "Efficient privacy-preserving access control of mobile multimedia data in cloud computing", IEEE Access, vol. 7, pp. 131534-131542, 2019.

13] R. Li, C. Shen, H. He, X. Gu, Z. Xu and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing", IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344-357, Apr. 2018.

14] S. Fugkeaw and H. Sato, "Scalable and secure access control policy update for outsourced big data", Future Gener. Comput. Syst., vol. 79, pp. 364-373, Feb. 2018.

15] S. Agrawal and R. D. Gupta, "Web GIS and its architecture: A review", Arabian J. Geosci., vol. 10, no. 23, pp. 1-13, Dec. 2017.