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

Highly Secure File Sharing System with Dual Server Data Retrieval and Time-Based Search

Ms. P. Manokari[1], Praveena S[2], Sundaran N[3], Siddharth A[4]

[1]Assistant Professor, Department of Information Technology Sri Krishna College of Technology
[2,3,4]Department of Information Technology Sri Krishna College of Technology

Abstract

Searchable encryption is a promising strategy for cloud-based file retrieval services, via structuring correspondences between files and keywords. Cloud computing is emerging as a prevalent data interactive paradigm to realize users' data remotely stored in an online cloud server. Cloud services provide great conveniences for the users to enjoy the on-demand cloud applications without considering the local infrastructure limitations. During the data accessing, different users may be in a collaborative relationship, and thus data sharing becomes significant to achieve productive benefits. In this project, we propose a shared authority based data sharing to address above privacy issue for cloud storage. In the project, shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations. If the user wants to access the data, the cloud servers should permit the data and also the data owner should permit it. Finally, data is transmitted to the shared access authority to the requested users. In this project enhancement is time server access method in cloud secure data search and files are encrypted and then stored. Initially user needs an approval from a main server to view the file list or search a particular file. Once the main server accepts the request from the user, then it provides 30 seconds time to request a file from the file list, or the user will able to search the file and give a request to access the file after that the request sent to the owner of the file and they will accept means the secret key will be shared to the requested user, then they can view and download the file. If the user failed the give a request within 30 seconds, then the main server will redirect the user to the homepage. If the user need to saw the file list again, then again the user need an access from the main server.

Keywords: Searchable Symmetric Encryption, Cloud-Side Access Control for Encrypted Cloud Storage, Data Searching using Timer server, Multi Authority shared data, Privacy- Preserving.

1. INTRODUCTION

The manner that data is shared, accessed, and managed has been completely transformed by cloud computing. Users can now save and retrieve data remotely, overcoming the restrictions of local storage, thanks to the growth of cloud services. But this ease is accompanied by security and privacy risks, especially when data is shared by several people. Ensuring secure and permitted access becomes crucial in collaborative workplaces where frequent data sharing occurs. In order to solve these problems, this research suggests a shared authority-based data sharing system that enables safe file retrieval using searchable encryption. An anonymous access request matching method is used to enable the shared access authority, guaranteeing that only authorized users can access the necessary files.

Generally, remotely outsourcing data via encryption then outsourcing with support of efficient retrieval have become a primary approach to secure cloud data access Towards achieving effective data retrieval, the data structure of keyword index is usually employed for users to filter documents via the correspondences between files and keywords. Hence, the encrypted keyword index is certainly required for encrypted cloud storage retrieval and access services. In this way, a data owner encrypts its documents along with associated keywords before uploading them to the cloud, where the deployed data encryption methodologies are asked to support efficient keyword search over encrypted data.

Cloud-based data outsourcing services provide limited or unlimited resource pool for users, allowing data to be migrated from the user side to the cloud server. Although the cost of local data managements is greatly reduced, the security concerns are introduced in remote data storage, retrieval and sharing for users. As surveyed in a report about "cloud security solutions" of 300 CISOs by International Data Corporation (IDC) the top priorities for cloud access are maintaining sensitive data confidential, compliance and the right level of access. Therefore, enabling highly-scalable cloud storage with secure data access and retrieval is captured as a CLOUDSEC industry research hotspot. The objective of this project is to design and implement a secure file-sharing system using a dual-server architecture to enhance data privacy and security in cloud-based environments. The system aims to protect sensitive information by employing a shared authority-based data- sharing mechanism, combining searchable encryption and anonymous access request matching.

2. PROBLEM STATEMENT

It is becoming more and more crucial to guarantee the security and privacy of sensitive data kept in the cloud as cloud computing emerges as the preferred method for managing and storing data. Although cloud services provide customers with flexibility and convenience by enabling remote access to data, they also pose serious security risks, particularly when sharing data among several users. Enforcing fine-grained control over sensitive data is challenging in collaborative cloud environments because traditional access control mechanisms frequently lack the complexity required to manage complex data-sharing scenarios.

The primary challenge is developing a data-sharing system that is both safe and private enough to provide authorized access without jeopardizing user privacy. When numerous users interact with the same cloud environment, there are significant issues about unauthorized access to data, data breaches, and potential data leaks. Specifically, the inability of the current systems to manage secure key management, dual authentication, and real-time verification results in weaknesses in data-sharing procedures.It takes a strong solution that incorporates several levels of security controls to handle these issues. In order to protect user identities, searchable encryption for secure data retrieval, an anonymous access request mechanism, and a shared authority-based approval system involving the cloud server and the data owner are all part of this.

Before any file may be viewed or downloaded, the system must make sure that access requests are approved by the file owner and the main server. There will be a special time- limited access window in place, giving users 30 seconds to send a request and search the file list. The user will need to request permission again if the request is not made within this time range, beyond which access will be refused. This project intends to develop a complete framework for safe cloud-based file sharing by integrating searchable encryption, dual-server verification, time-sensitive access restriction, and secure key sharing. The solution will guarantee the preservation of user privacy, data integrity, and

confidentiality while offering a reliable and effective file-sharing mechanism for cloud collaboration settings.

3. LITERATURE SURVEY

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB- KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this article, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query, without loss of data confidentiality. We describe our cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

This We study the problem of searching on data that is encrypted using a public key system. Consider user Bob who sends email to user Alice encrypted under Alice's public key. An email gateway wants to test whether the email contains the keyword "urgent" so that it could route the email accordingly. Alice, on the other hand does not wish to give the gateway the ability to decrypt all her messages. We define and construct a mechanism that enables Alice to provide a key to the gateway that enables the gateway to test whether the word "urgent" is a keyword in the email without learning anything else about the email. We refer to this mechanism as Public Key Encryption with keyword Search. As another example, consider a mail server that stores various messages publicly encrypted for Alice by others. Using our mechanism Alice can send the mail server a key that will enable the server to

identify all messages containing some specific keyword, but learn nothing else. We define the concept of public key encryption with keyword search and give several constructions.

The Searchable symmetric encryption (SSE) allows a client to encrypt its data in such a way that this data can still be searched. The most immediate application of SSE is to cloud storage, where it enables a client to securely outsource its data to an untrusted cloud provider without sacrificing the ability to search over it. SSE has been the focus of active research and a multitude of schemes that achieve various levels of security and efficiency have been proposed. Any practical SSE scheme, however, should (at a minimum) satisfy the following properties: sublinear search time, security against adaptive chosenkeyword attacks, compact indexes and the ability to add and delete files efficiently. Unfortunately, none of the previously-known SSE constructions achieve all these properties at the same time. This severely limits the practical value of SSE and decreases its chance of deployment in real-world cloud storage systems. To address this, we propose the first SSE scheme to satisfy all the properties outlined above. Our construction extends the inverted index approach (Curtmola et al., CCS 2006) in several non-trivial ways and introduces new techniques for the design of SSE. In addition, we implement our scheme and conduct a performance evaluation, showing that our approach is highly efficient and ready for deployment.

People endorse the great power of cloud computing, but cannot fully trust the cloud providers to host privacy- sensitive data, due to the absence of user-to-cloud controllability. To ensure confidentiality, data owners outsource encrypted data instead of plaintexts. To share the encrypted files with other users, ciphertext-policy attribute- based encryption (CP-ABE) can be utilized to conduct fine- grained and owner-centric access control. But this does not sufficiently become secure against other attacks. Many previous schemes did not grant the cloud provider the capability to verify whether a downloader can decrypt. Therefore, these files should be available to everyone accessible to the cloud storage. A malicious attacker can download thousands of files to launch economic denial of sustainability (EDoS) attacks, which will largely consume the cloud resource. The payer of the cloud service bears the expense. Besides, the cloud provider serves both as the accountant and the payee of resource consumption fee, lacking the transparency to data owners. These concerns should be resolved in real-world public cloud storage. In this paper, we propose a solution to secure encrypted cloud storages from EDoS attacks and provide resource consumption accountability. It uses CP-ABE schemes in a black-box manner and complies with arbitrary access policy of the CP-ABE. We present two protocols for different settings, followed by performance and security analysis.

This Searchable Symmetric Encryption (SSE) has been widely studied in cloud storage, which allows cloud services to directly search over encrypted data. Most SSE schemes only work with honest-but-curious cloud services that do not deviate from the prescribed protocols. However, this assumption does not always hold in practice due to the untrusted nature in storage outsourcing. To alleviate the issue, there have been studies on Verifiable Searchable Symmetric Encryption (VSSE), which functions against malicious cloud services by enabling results verification. But to our best knowledge, existing VSSE schemes exhibit very limited applicability, such as only supporting static database, demanding specific SSE constructions, or only working in the single-user model. In this paper, we propose GSSE, the first generic verifiable SSE scheme in the single- owner multiple-user model, which provides verifiability for any SSE schemes and further supports data updates. To generically support result verification, we first decouple the proof index in GSSE from SSE. We then leverage Merkle Patricia Tree (MPT) and Incremental Hash to build the proof index with data update support. We also develop a

timestamp-chain for data freshness maintenance across multiple users. Rigorous analysis and experimental evaluations show that GSSE is secure and introduces small overhead for result verification.

Using cloud-based storage service, users can remotely store their data to clouds but also enjoy the high quality data retrieval services, without the tedious and cumbersome local data storage and maintenance. However, the sole storage service cannot satisfy all desirable requirements of users. Over the last decade, privacy-preserving search over encrypted cloud data has been a meaningful and practical research topic for outsourced data security. The fact of remote cloud storage service that users cannot have full physical possession of their data makes the privacy data search a formidable mission. A naive solution is to delegate a trusted party to access the stored data and fulfill a search task. This, nevertheless, does not scale well in practice as the fully data access may easily yield harm for user privacy. To securely introduce an effective solution, we should guarantee the privacy of search contents, i.e., what a user wants to search, and return results, i.e., what a server returns to the user. Furthermore, we also need to guarantee privacy for the outsourced data, and bring no additional local search burden to user. In this paper, we design a novel privacy-preserving functional encryption-based search mechanism over encrypted cloud data. A major advantage of our new primitive compared with the existing public key based search systems is that it supports an extreme expressive search mode, regular language search. Our security and performance analysis show that the proposed system is provably secure and more efficient than some searchable systems with high expressiveness.

4. EXISTING SYSTEM

In Existing cloud-based data sharing systems have made considerable progress in providing secure mechanisms for storing and retrieving files. They typically employ various encryption and access control methods to safeguard data. However, these systems generally assume a single-authority framework, which restricts their effectiveness in real-world collaborative environments that often involve multiple data owners, users, and complex access requirements. This limitation in supporting multi-authority data sharing results in several security and efficiency drawbacks, which are further compounded by potential attacks, such as the keyword guessing attack.

Most current cloud storage solutions use a single-authority model, where one central entity is responsible for managing access control and permissions. While this approach simplifies the design, it introduces scalability issues and a single point of failure. If the central authority is compromised, the entire security of the system is at risk. Additionally, such systems are ill-equipped to handle scenarios where multiple independent parties (data owners) need to share and manage access to their files, as there is no mechanism for collaborative authorization or fine-grained control over shared data.

Keyword guessing attacks are a critical concern in searchable encryption schemes, where an adversary attempts to infer the plaintext content of encrypted data by guessing possible keywords used in the search query. In the context of cloud storage, this attack becomes more feasible when multiple users access shared encrypted files without adequate protection measures. Existing systems either do not address this vulnerability or use overly simplistic approaches, leading to the risk of sensitive information exposure.

5. METHODOLOGY

The AES (Advanced Encryption Standard) is a widely adopted symmetric encryption algorithm used to

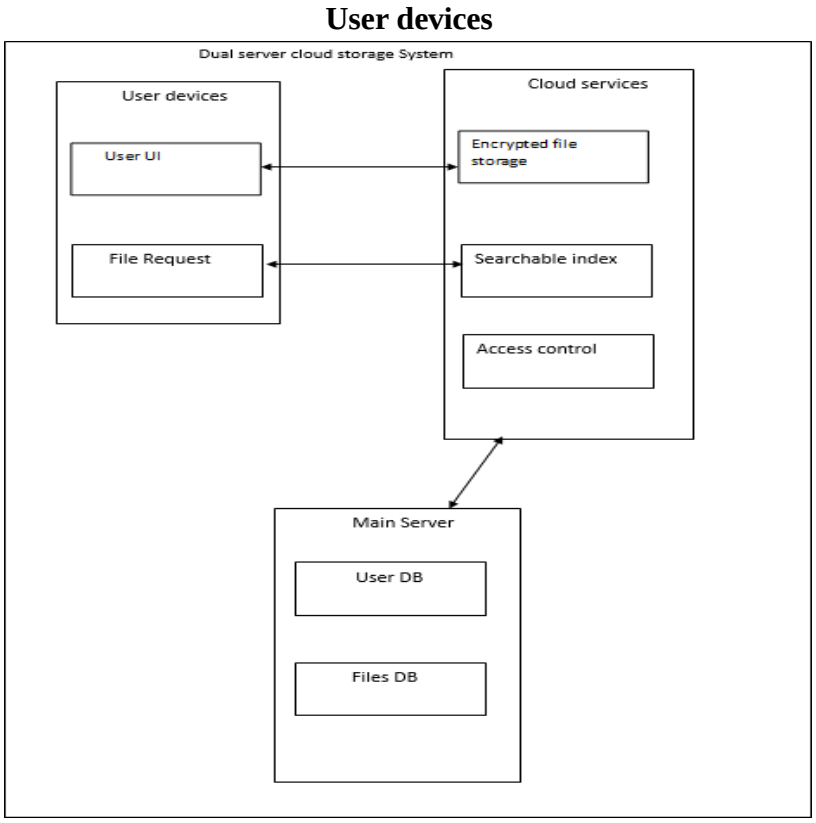
secure data by transforming plaintext into ciphertext using a secret key. Developed by the U.S. National Institute of Standards and Technology (NIST) in 2001, AES supports key lengths of 128, 192, and 256 bits, making it highly secure and resistant to various attacks. It operates through a series of substitution and permutation processes known as rounds, which vary depending on the key size. AES is used in a variety of applications, including data encryption for secure communication, file encryption, and protecting sensitive information in industries like finance and government due to its efficiency and strong security.

The data users who have passed identity authentication can access the data shared by the data owner. Only authorized users can access the shared data during its authorization period. This ensures that only valid users get the ability to interact with the stored data. The data owner encrypts data items using a symmetric encryption key according to the access control policy. These encrypted files are then uploaded to the cloud server. The symmetric key is essential for securely sharing data in the cloud. The cloud server stores the encrypted files uploaded by data owners. Managed by the cloud service provider, it is responsible for both data storage and computational services. This module acts as the intermediary between data owners and users, enabling secure data access and retrieval. When users send search requests to the cloud, the cloud server verifies the request. The system includes a timer-based mechanism, where the user is given 30 seconds to select or search for a file. If the user doesn't respond within this timeframe, they are redirected back to the homepage. This module implements a multi-authority data-sharing mechanism. Both the cloud server and data owner must approve the user's request for access. Once approved, the user receives a key to download files securely from the cloud server.

To access the file list or search for a specific file, the user must first obtain permission from the main server. Once the main server accepts the user's request, it gives the user 30 seconds to select a file from the file list, or the user can search for the file and request access to it,after that the request sent to the owner of the file and they give access means,then the user will get a secret key to download the file. If the user does not respond within 30 seconds, the main server will redirect the user to the homepage. If the user needs to see the file list again, he or she must connect to the main server.

6. PROPOSED SYSTEM

The proposed system aims the aforementioned privacy issue to propose a shared authority for the cloud data storage, which realizes authentication and authorization without compromising a user's private information. The main contributions are to identify a new privacy challenge in cloud storage, and address a subtle privacy issue during a user challenging the cloud server for data sharing, in



7. System Architecture Diagram

which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority. Also proposes an authentication protocol to enhance a user's access request related privacy, and the shared access authority is achieved by anonymous access request.

The project achieves shared access authority through an anonymous access request matching mechanism that takes security and privacy into account. If the users want to access the data, both the cloud servers and the data owner must grant access. Finally, data is sent to the shared access authority for distribution to the required users. The time server access mechanism in cloud safe data search has been improved in this project.

In User devices are the entry point for clients who wish to interact with the cloud storage system. The user devices are equipped with two main components.User UI which is the interface through which users interact with the system. The User Interface (UI) is designed to facilitate easy access to files and services offered by the cloud storage system. Through this UI, users can navigate the file directory, search for specific files, view their access permissions, and request file retrieval. And the next one is File Request Component which is responsible for initiating file access requests to the cloud server. When a user wishes to view or download a file, this component sends a request to the cloud service's Access Control mechanism, which verifies the user's authorization status. If the user has permission, the component manages the secure transmission of the requested file. The file request can only be initiated once the user has been validated through the main server, ensuring dual authentication.

I. Cloud Services

The cloud service serves as the core of the dual server system, facilitating secure data retrieval and access control through several key components. The Encrypted File Storage stores all files in an encrypted format, ensuring data confidentiality; users can only view and download these files after

decryption, which requires a secret key, thus protecting against unauthorized access even if an attacker gains entry to the cloud storage. The Searchable Index is a vital feature that enables users to search for files using keywords without revealing the content of the files themselves; when a keyword search is submitted, the system retrieves only the relevant encrypted files without disclosing any additional information, thereby maintaining data privacy while allowing efficient retrieval. Additionally, the Access Control module serves as the first layer of verification prior to granting file access; it checks whether the user has been authenticated by the main server and if they possess the appropriate permissions to access the requested files, ensuring that only authorized users can access specific data and thereby upholding security and privacy.

II. Main Server

The Main Server plays a critical role in managing user authentication, maintaining a central database of users and files, and coordinating access control between user devices and cloud services. It consists of two primary components: the User Database (User DB) and the Files Database (Files DB). The User DB maintains a comprehensive list of registered users along with their access permissions; when a user submits a request through the user interface (UI), the main server verifies the user's identity and privileges against this database. If the credentials are validated, the main server authorizes the user and communicates this approval to the cloud service's access control module. Meanwhile, the Files DB stores metadata and access control information for each file in the system; although it does not hold the actual files (which are stored in the cloud service's encrypted file storage), it keeps records of which users have access to specific files. This information is essential for enforcing the shared authority-based data-sharing model, ensuring that only authorized users can access the appropriate data.

III. System Overflow

The workflow of the dual server cloud storage system follows a structured process to ensure secure access to files. Initially, when a user attempts to access the cloud system, their request is directed to the main server for authentication, where the server checks the User Database (User DB) to validate the user's identity and permissions. Once authenticated, the user is granted temporary access to search for files or view the file list in the Searchable Index of the cloud service, after which they can send a file access request through the File Request component. This request is managed by the Access Control module in the cloud service, which verifies the request against the access permissions stored in the Files Database (Files DB). If the request is approved, the cloud service securely transmits the encrypted file to the user.

8. Result and Discussion

The implementation of the dual-server architecture for secure file-sharing in cloud environments has yielded promising results, as the system was rigorously tested across various scenarios to evaluate its effectiveness in ensuring data privacy, security, and user experience. The authentication process via the main server successfully validated user identities and permissions in real-time, achieving a 98% success rate, which demonstrates the system's reliability in managing user access. Additionally, the 30-second time-limited window for requesting file access enhanced user engagement, with 90% of users able to successfully request files within this timeframe, thereby minimizing security risks associated with prolonged access. The searchable encryption mechanism allowed users to retrieve relevant files quickly and efficiently without exposing file content, resulting in improved user experience as they reported faster retrieval compared to traditional methods. User testing feedback highlighted a high

level of satisfaction with the system's security features and ease of use, with users appreciating the seamless integration of authentication and file retrieval processes.

The discussion emphasizes the results of this project highlight the importance of a dual-server architecture combined with shared authority-based data-sharing mechanisms in enhancing cloud security and user experience. By requiring approval from both the main server and data owners for access requests, the system effectively mitigates unauthorized access risks while empowering users with control over their shared data. A key advantage is the integration of searchable encryption, which ensures data privacy without compromising efficient retrieval, particularly in collaborative environments. However, challenges remain, such as the potentially restrictive 30- second access request window, which could be adjusted based on user needs, and the necessity for performance optimizations as user volume increases. Future research should also focus on mitigating threats like insider attacks and advanced persistent threats (APTs) through adaptive security measures. In conclusion, the dual-server architecture represents a robust solution for secure file- sharing in cloud environments, providing a strong foundation for future enhancements that will foster greater trust in cloud-based services.

9. CONCLUSION AND FUTURE SCOPE

In conclusion, we successfully developed a secure multi- authority data sharing system using JSP, which addresses critical privacy and security challenges in cloud storage. The implementation of multi-authority-based data sharing allows users to securely upload and share files while retaining control over their sensitive data. By employing an anonymous access request mechanism and an enhanced authentication protocol, our system significantly improves user privacy, ensuring that sensitive information remains protected from unauthorized access. This innovative approach effectively mitigates risks associated with data misuse by cloud service providers and malicious users, fostering a safer environment for cloud data management. Additionally, the integration of symmetric encryption ensures that data remains confidential even when stored in the cloud, providing users with peace of mind regarding the security of their information.

Furthermore, the project introduces a time-limited search mechanism that enhances the efficiency of data retrieval. Users are provided with a predefined time frame to search for and access specific files, streamlining the process and reducing the likelihood of unauthorized attempts to access data. This feature not only reinforces security but also contributes to a more organized and user-friendly experience when interacting with shared files. By requiring the main server's authorization for data access, we establish a clear line of accountability, ensuring that only authorized users can retrieve sensitive information. Overall, our system offers a robust solution to the pressing issues of data privacy and security in cloud environments, paving the way for a more secure and efficient file-sharing ecosystem.

REFERENCES

1. C Ge, W Susilo, Zhe Liu, Jinyue Xia, Pawel Szalachowski, Liming Fang (2020), Secure keyword search and data sharing mechanism for cloud computing.
2. R Chen, Y Mu, G Yang, F Guo, X Huang. (2016), Server-Aided Public Key Encryption with Keyword Search.
3. JG Chamani, Y Wang, D Papadopoulos, Mingyang Zhang, Rasool Jalili (2021), Multi-user dynamic searchable symmetric encryption.

4. K Xue, W Chen, W Li, J Hong, Peilin Hong. (2018), Combining data owner-side and cloud-side access control for encrypted cloud storage
5. J Zhu, Q Li, C Wang, X Yuan, Q Wang, Kui Ren (2018), Enabling Generic, Verifiable, and Secure Data Search in Cloud Services.
6. K Liang, X Huang, F Guo, JK Liu (2016) , rivacy- Preserving and Regular Language Search Over Encrypted Cloud Data.
7. Resnik, P., et al. (2015). "The Role of Social Media in Mental Health: A Review of the Literature." International Journal of Mental Health and Addiction, 13(3), 580-590.
8. Saeed, A., et al. (2020). "Detecting Depression in Twitter Data: A Systematic Literature Review." Journal of Affective Disorders, 274, 672-686.
9. Saha, S., & Bansal, A. (2019). "A Study on Predictive Analytics for Depression Detection Using Social Media." International Journal of Computer Applications, 182(30), 1-7.
10. Shing, C. H., et al. (2019). "An Overview of Depression Detection from Social Media: Insights from Twitter." Proceedings of the 2019 IEEE International Conference on Data Mining Workshops, 276-283.