International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 2, Mar-Apr-2019, ISSN (Online): 2395-566X

A Review on Analysis of Data Search Scheme for Secure Information Retrieval in Cloud Computing

M.Tech. Scholar Nitin Kumar Sahu
BIRT Bhopal
Bhopal, MP, India
sahu.nitin2803@gmail.com

Asst. Prof. Anuj Kumar Pal
BIRT Bhopal
Bhopal, MP, India
junaamity@gmail.com

Abstract- **Today's businesses want it all: secure data and applications accessible anywhere from any device. It's possible with cloud technology, but there are inherent challenges to making it a reality. What can enterprise businesses do to reap the benefits of cloud technology while ensuring a secure environment for sensitive information? Recognizing those challenges is the first step to finding solutions that work. . Increasingly numerous companies plan to move their local data management systems to the cloud and store and manage their product information on cloud servers. An accompanying challenge is how to protect the security of the commercially confidential data, while maintaining the ability to search the data. In this paper we are analysis of different securities scheme for encryption of item information and also for data search scheme in cloud computing.**

Keywords- **clound computing, cloud security, security issues, Information security.**

I. INTRODUCTION

As large amounts of data are outsourced to cloud storage servers, the need for data owners to encrypt the abovementioned second and third types of sensitive data makes traditional plain text-based data search solutions no longer suitable. In addition, restricted by the network bandwidth and local storage capacity constraints, users find it impossible to re-download all the data to a local disk and later decrypt them for use. Based on the above issues, privacy-preserving data search schemes were born, designed to ensure that only legitimate users based on identifiers or keywords, and have the ability to search the data. These schemes safeguard the users' personal data but enable the server to return to the target cipher text file according to the query request. Thus, we can ensure the security of user data and privacy while not unduly reducing the query efficiency.

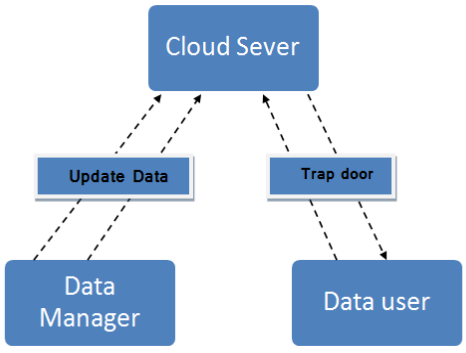

Figure 1 Encrypted information retrieval system model

As large amounts of data are outsourced to cloud storage servers, the need for data owners to encrypt the abovementioned second and third types of sensitive data makes traditional plain text-based data search solutions no longer suitable. In addition, restricted by the network bandwidth and local storage capacity constraints, users find it impossible to re-download all the data to a local disk and later decrypt them for use. Based on the above issues, privacy-preserving data search schemes were born, designed to ensure that only legitimate users based on identifiers or keywords, and have the ability to search the data. These schemes safeguard the users' personal data but enable the server to return to the target cipher text file according to the query request. Thus, we can ensure the security of user data and privacy while not unduly reducing the query efficiency.

II. RELATED WORK

Ying-si zhao et al. [1] "**Secure and Efficient Product Information Retrieval in Cloud Computing**" In this paradigm Cloud computing is a promising information technique that can organize a large amount of IT resources in an efficient and flexible manner. Increasingly numerous companies plan to move their local data management systems to the cloud and store and manage their product information on cloud servers. An accompanying challenge is how to protect the security of the commercially confidential data, while maintaining the ability to search the data. In this paper, a privacy-preserving data search scheme is proposed, that can support both the identifier-based and feature-based product searches. Specifically, two novel index trees are constructed and encrypted, that can be searched without knowing the plaintext data. Analysis and simulation results demonstrate the security and efficiency of our scheme.

ZHEN WANG et al**.** [2] **" Enhanced Instant Message Security and Privacy Protection Scheme for Mobile Social Network Systems"** The proposed scheme supports denial of replaying attack and denial of forgery attack by utilizing timestamps and the elliptic curve digital signature algorithm. It supports multiple types of messages (such as document and multimedia messages) and prevents privacy leakage by storing sent and received messages with cipher text. We proved the security of the proposed scheme under the elliptic curve discrete logarithm assumption and the CDH assumption. The comparison results of the proposed scheme with other schemes and the results of an experiment show that it is a comprehensive secure scheme with high security and good practicability.

Cao et al. [3] first proposed a basic privacy-preserving multi-keyword ranked search scheme based on a secure kNN algorithm [26]. A set of strict privacy requirements are established, and two schemes are later proposed to improve the security and search experience. However, an apparent drawback of this scheme is that the search efficiency is linear with the cardinality of the document collection, and consequently, it cannot be used to process extremely large document databases.

Xia et al. [4] designed a keyword balanced binary tree to organize the document vectors and proposed a ''Greedy Depth-First Search'' algorithm to improve the search efficiency. Moreover, the index tree can be updated dynamically with an acceptable communication burden.
Yusof et al. [10] applied a hash algorithm in a secure module of an IM system to encrypt and convert the data into hash values, which can ensure that unauthorized persons cannot view the original data through the network. However, it is not sufficiently secure for IM system to use only a hash algorithm in a secure module. For instant text messaging in mobile devices,

Akhilesh Yadav et al. "Securing Cloud Computing Environment using Quantum Key Distribution" Nowadays, Information Technology group is undergone significant shift in computing and protecting business value by using well-built, workable and authentic replacement of Cloud Computing. Cloud Computing is a contemporary computational architecture that provides another type of model. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the security issues of cloud computing and the role of cryptography technique in Cloud computing to enrich the Information Security.

Rongzhi Wang "Research on Data Security Technology Based on Cloud Storage" Encryption storage, Integrity verification, access control and verification and so on. Through the data segmentation and refinement rules algorithm to optimize the access control strategy, using the data label verification cloud data integrity, using replica strategy to ensure the data availability, the height of authentication to strengthen security, attribute encryption method using signcryption technology to improve the algorithm efficiency, the use of time encryption and DHT network to ensure that the cipher text and key to delete the data, so as to establish a security scheme for cloud storage has the characteristics of privacy protection.

III. CLOUD SECURITY CHALLENGES

1. DDoS attacks

As more and more businesses and operations move to the cloud, cloud providers are becoming a bigger target for malicious attacks. Distributed denial of service (DDoS) attacks is more common than ever before. Verisign reported IT services, cloud and SaaS was the most frequently targeted industry during the first quarter of 2015. A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests.

If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.**N**Complementing cloud services with DDoS protection is no longer just good idea for the enterprise; it's a necessity. Websites and web-based applications are core components of 21st century business and require state-of-the-art security.

2. Data breaches

Known data breaches in the U.S. hit a record-high of 738 in 2014, according to the Identity Theft Research Center, and hacking was (by far) the number one cause. That's an incredible statistic and only emphasizes the growing challenge to secure sensitive data. Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in private, public and hybrid scenarios), some of those controls are relinquished to a trusted partner. Choosing the right vendor, with a strong record of security, is vital to overcoming this challenge.

3. Data loss

When business critical information is moved into the cloud, it's understandable to be concerned with its security. Losing data from the cloud, either though accidental deletion, malicious tampering (i.e. DDoS) or an act of nature brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data. To face this challenge, it's imperative to ensure there is a disaster recovery process in place, as well as an integrated system to mitigate malicious attacks. In addition, protecting every network

layer, including the application layer (layer 7), should be built-in to a cloud security solution.

5. Insecure access points

One of the great benefits of the cloud is it can be accessed from anywhere and from any device. But, what if the interfaces and APIs users interact with aren't secure? Hackers can find these types of vulnerabilities and exploit them. A behavioral web application firewall examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications from security breaches.

6. Notifications and alerts

Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough security plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

IV. PROPOSED WORK

- A product information outsourcing and searching system model including the data owner, cloud server and data users is designed.
- Two index structures supporting efficient product retrieval are constructed. Moreover, corresponding search algorithms are also proposed
- Cloud storage auditing protocol with secure outsourcing of key updates is composed by seven algorithms (SSetup, EUpdate, VESK, DESK, AuthGen, Proof- Gen, Proof Verify and Check Proxy TPA), shown below:
- SSetup: the system setup algorithm is run by the client. It takes as input a security parameter k and the total number of time periods T, and generates an encrypted initial client's secret key ESK0, a decryption key DK and a public key PK. Finally, the client holds DK, and sends ESK0 to the TPA.
- EUpdate: the encrypted key update algorithm is run by the TPA. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, and generates a new encrypted secret key ESKj+1 for period j + 1.
- VESK: the encrypted key verifying algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , the current period j and the public key PK, if ESKj is a well-formed encrypted client's secret key, returns 1; otherwise, returns 0.
- DESK: the secret key decryption algorithm is run by the client. It takes as input an encrypted client's secret key ESKj , a decryption key DK, the current period j and the public key PK, returns the real client's secret key SKj in this time period.
- AuthGen: the authenticator generation algorithm is run by the client. It takes as input a file F, a client's secret key SKj , the current period j and the public key PK, and generates the set of authenticators _ for F in time period j.
- ProofGen: the proof generation algorithm is run by the cloud. It takes as input a file F, a set of authenticators a challenge a time period j and the public key PK, and generates a proof P which proves the cloud stores F correctly.
- Checking algorithm for proxy server of TPA Proof Verify: the proof verifying algorithm is run by the TPA. It takes as input a proof P, a challenge a time period j, and the public key PK, and returns
- A series of simulations are conducted to illustrate the security and efficiency of the proposed scheme.

V. CONCLUSION

In this paper, we designed a secure and efficient product information retrieval scheme based on cloud computing. Specifically, two index structures, including a hash value AVL tree and a product vector retrieval tree, are constructed, and they support an identifier-based product search and feature-vector-based product search, respectively. By checking a proxy server we will find out the fault in encryption. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the client end and the cloud server end. Main goal of cloud computing is securely store and transmit the data in cloud

REFERENCES

[1] YING-SI ZHAO "Secure and Efficient Product Information Retrieval in Cloud Computing" Received February 10, 2018, accepted March 11, 2018, date of publication March 19, 2018, date of current version April 4, 2018

[2] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. ESpafford, "Secure outsourcing of scientific computations," Trends in Software Engineering, vol. 54, pp. 215-272

[3] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2010.

[4] Younis A. Younis, Kashif Kifayat, Madjid Merabti, "An access control model for cloud computing", Elsevier journal of information security and applications, 2014.

[5] C. Wang, Q. Wang, K. Ren, N. Cao, W. LouToward secure and dependable storage services in cloud computing IEEE Trans. Services Comput., 5 (2) (2012), pp. 220-232

[6] Duncan, Adrian, Sadie Creese, and Michael Goldsmith . "Insider attacks in cloud computing." Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE,2012.