International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-6, April 2020

A Secure Data Storage Strategy for Private Cloud

G. Nagi Reddy, P. Satya Shekar Varma

Abstract*: In recent years, with the widespread application of cloud computing, more and more enterprises, institutions, and individuals have started to use cloud services to place their data in the cloud. With the rise of cloud services, the accompanying data security issues have received increasing attention. Because data stores are in the cloud, there are many outstanding security issues. This paper proposes a public cloud data security solution based on a trusted third-party platform. The solution is based on an independent and trusted third-party platform, and has certain advantages in data encryption, key management, data awareness, data sharing, and accident responsibility.

***Keywords* : Cloud, Cloud Computing, Cloud Data Security, Private Cloud, Security.**

I. INTRODUCTION

Cloud Computing is an Internet-based computing method. It consists of a series of resources that can be dynamically upgraded and virtualized. These resources are shared by all users of cloud computing and can be easily accessed through the network. Users do not need to master Cloud computing technology only needs to lease cloud computing resources according to the needs of individuals or groups. As shown in Fig. 1, cloud computing is generally divided into the following three categories: IaaS (Infrastructure as a Service, Infrastructure as a Service), PaaS (Platform as a Service, Platform as a Service), SaaS (Software as a Service, Software ie Service) [1]. Public cloud (or open cloud), simply explained, is that third parties provide services directly to external users through their own infrastructure. External users access services through the Internet and do not own cloud computing resources. The public cloud has solved the problems in the informatization process of some small and medium-sized enterprises with insufficient resources by reducing costs, improving efficiency, and professional operation and maintenance. However, the above shortcomings of the public cloud hinder the development of the public cloud, as shown in Fig. 2.

The Faced with security flaws in public clouds, private clouds have emerged. It is built for one user's sole use, that is, a closed, exclusive cloud for the user's own use.

Revised Manuscript Received on April 30, 2020.
***** Correspondence Author
G. Nagi Reddy, Department of Computer Science and Engineering at Mahatma Gandhi Institute of Technology, Hyderabad, India. E-mail: gnagireddy_cse@mgit.ac.in
P. Satya Shekar Varma*, Department of Computer Science and Engineering at Mahatma Gandhi Institute of Technology, Hyderabad, India. E-mail: pssvarma_cse@mgit.ac.in.

Users have all the infrastructure of cloud computing (i.e. server clusters), which can be deployed inside the firewall in the data center, or they can be deployed in a secure colocation site. In general, in order to enjoy the convenience of cloud computing while ensuring data security, some companies will build their own private clouds and place them under internal protection.

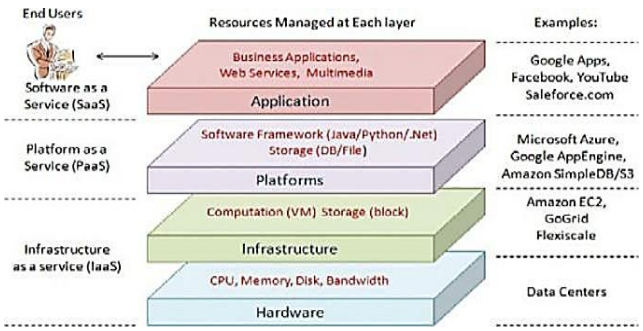

Fig. 1. Cloud service architecture.

Private clouds can be very good at securing data, but it also has some fatal flaws:

- The construction cost is high, and some small and medium enterprises and individual users cannot afford to set up.
- The scalability is poor, and the cost is higher when the technology is updated or resources are insufficient to expand.
- The resource capacity and computing power are not comparable to public clouds.

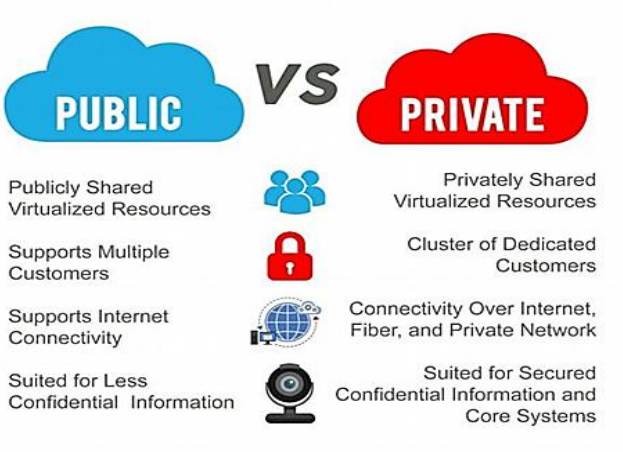

Fig. 2. Comparison of public and private clouds.

In present years, with the rise of c-computing, diverse cloud provider providers have sprung up, and more and more organizations, institutions and individuals have all started to keep their records within the cloud, taking advantage of the big facts capability and excessive Computing pace can remedy many issues. However, at the equal time,

the tremendous software of cloud computing has also brought many new safety dangers. The most prominent one is the data security issue. The cloud application has changed the traditional data management model, and a large amount of data is stored on cloud servers that are not controlled by users. At the same time, due to the different technical levels and management systems of various cloud service providers, it is difficult for users to know who is a reliable cloud service provider. In addition, due to the lack of uniform enforcement standards in the industry on how to store and protect data, and the companies currently providing cloud computing services generally lack adequate protection measures against external attacks and data security leaks, there are general flaws in data security.

In the year 2012, the well-known employer VMware introduced the 1/3 annual cloud warmth survey. 70% of customers refused to undertake the cloud, in particular due to issues about cloud facts protection and privacy protection. This indicates that safety and private ness problems have grow to be the biggest limitations to the development of cloud services [4]. In response to this problem, this article proposes a set of public cloud data security solutions based on trusted third-party platforms. The solution is based on independent trusted third-party platforms, covering data encryption, key management, data awareness, data sharing, Key technologies such as the identification of accident responsibilities, to some extent, solve public cloud data storage security issues.

II. STATUS OF CLOUD DATA STORAGE

A. Analysis of Key Issues in Cloud Data

The most prominent issue in cloud security is data security, although every cloud service provider claims that its services are very secure in all aspects. But for enterprises, especially large enterprises, business- related data is their lifeline and cannot be threatened in any form. Especially since the incident of SONY data leakage, cloud data security has once again become the focus of attention.

Security is an important issue for every user. Cloud computing is based on the communication network, and the network itself has many insecure factors. When a user puts data on the cloud, the cloud is a virtual environment. The user does not know where the data is, who is using the cloud, who is controlling the cloud. The application environment and data are out of the user's control. These are Cloud insecurities [5].

The data security issues generated by the cloud environment are mainly as follows:

- *Privacy of data:* With the rapid development of cloud computing, people's understanding of cloud storage has gradually deepened. Whether it is some enterprises or some individuals, data has been stored in the cloud. However, the security of data storage in the cloud is thought-provoking. For individual users, he may store his photos, contacts, chats, personal files, etc. in the cloud. If these private data are leaked, he may cause himself unnecessary trouble. For enterprise users, the information stored in the cloud is likely to involve trade secrets. If it is leaked, it will bring a major blow to the development of the enterprise. In addition, some government agencies are also trying to use cloud services. If their data is leaked, the consequences will be more serious.
- *Data perception and controllability:* Unlike traditional data storage, cloud data storage has almost unlimited computer resources, almost ubiquitous services, and almost unlimited storage space. This is the advantage of cloud services. However, because of these, users cannot know whether these resources and services are credible, cannot sense the existence of their own data, and cannot control their own data. In particular, it is impossible to know whether their data has been tampered with or copied illegally.
- *Secret sharing:* An important attribute of data in the cloud environment is sharing. In the process of using cloud services, users will use multiple forms of data sharing: some users need to share their data on multiple terminal devices, and some users need to share their data with colleagues. Share some work materials between them. At the same time, most of these shared data are private and cannot be leaked out of the sharing circle. Therefore, the cloud needs to be able to perform controlled sharing while maintaining privacy [6].
- *Loss of important data:* When an earthquake, fire, or human error occurs in the cloud service center, important data may be lost. However, at present, the multi-cloud data storage basically adopts a multi-point backup strategy. Data loss is also a case. Therefore, data loss is caused by this reason. The possibility of loss is generally small, and this factor is not considered in the design of cloud data secure storage solutions.
- *Accidental data loss responsibility determination:* Due to the particularity of electronic forensics in the cloud environment, when accidents such as data loss and data theft occur, it is often impossible to effectively determine liability. And now there is no official law to protect the privacy of cloud platform users, so that the data stored by users in the cloud loses its due security [7].

B. Cloud Data Security Threat Analysis

In the cloud environment, the threat of data security mainly comes from the following two aspects:

- One is that malicious administrators steal data. Since the data in the cloud environment is stored on the cloud service provider's cloud server, the data "ownership" is actually in the hands of the cloud service provider, and all data can be easily viewed by the cloud service provider. Therefore, if the internal management of the cloud service provider is not strict, and the cloud administrator has too much authority, or the cloud service provider itself has a malicious attempt, the data stored by the user in the cloud may be obtained by the administrator "legally".
- The second is hacking to steal data. In traditional data storage, corporate data is stored in its own internal network, protected by firewalls and security managers, while individual users store the data on their own hard drives. These ways of saving data are user-controllable, and the data has less chance of contact with the external environment. Because the cloud is an open environment, and the technical level of different cloud service providers may be different, the servers in the cloud are likely to be hacked, resulting in data loss.

III. CLOUD PLATFORM DESIGN SCHEME BASED ON TRUSTED THIRD PARTIES

A. Key Problem-Solving Ideas

1) Data Encryption

In order to ensure the security of data in the cloud, the data stored in the cloud needs to be encrypted. In order to take advantage of the strong computing power of the cloud, you can consider placing data encryption operations in the cloud and using a stronger encryption algorithm without worrying too much about encryption efficiency. This scheme uses two algorithms: RSA asymmetric encryption and AES symmetric encryption.

The Ron Rivest Securing Algorithm encryption algorithm is an uneven encryption set of rules. It is extensively used in public key encryption and electronic trade. The Ron Rivest Securing Algorithm generates a pair of public and private keys that cannot be calculated from each other. The public key is generally used for encryption, and the private key can decrypt data encrypted with the public key. AES (Advanced Encryption Standard) Advanced Encryption Standard, also known as Rijndael encryption method, is an encryption algorithm used to replace the original DES, which has been analyzed by many parties and widely used throughout the world. AES is an iterative, symmetric-key block cipher that uses 128, 192, and 256 -bit keys, and encrypts and decrypts data in 128-bit (16-byte) blocks. It has become one of the most popular algorithms in symmetric key encryption in 2006 [8]. By using these two encryption algorithms reasonably, cloud data can be encrypted to ensure data security.

2) Encryption Strategy

The use of different encryption strategies will have different impacts on data security and encryption performance. In order to make reasonable use of cloud computing resources and meet the needs of different users, this solution proposes two different encryption strategies. In actual applications, users can Need to choose the corresponding encryption strategy.

- *Encryption strategy based on AES algorithm:* The AES algorithm is used to encrypt cloud data. To ensure data security, a single key is not used. For each file and each field in the database, a randomly generated different key is used for encryption. Keep the keys in a separate module. This encryption strategy is characterized by high efficiency and fast encryption speed, but its security is relatively weak. Due to the use of symmetric keys, data will be easily stolen once the key is intercepted on the network. Therefore, the storage and use of the key (that is, data encryption and decryption) must be performed in the same place to prevent the key from being intercepted during network transmission.
- *One-time one-crypto encryption strategy based on RSA algorithm:* The Ron Rivest Securing algorithm is an asymmetric encrypting algorithm. In the application, a pair of public and private keys will be generated. The public key can be used to encrypt the data and stored in the cloud. When the data needs to be read, the private key is used to decrypt it.

The RSA algorithm is much more secure than the AES algorithm, but it also has some serious issues:

- The encryption speed is not high. When the data to be encrypted is relatively large, the speed of the RSA algorithm is obviously inferior to the AES algorithm.
- Although the RSA algorithm uses asymmetric keys, if the private key used to decrypt the data is intercepted, the data will also be stolen.

Therefore, in the R SA encryption strategy, if the encrypting and decrypting module it located in cloud, the powerful computing resources of the cloud can be used to make up for the shortcoming of the low speed of the R SA algorithm. However, the private key needs to be sent to the cloud for decryption each time it is decrypted. There is a possibility of interception. If the encryption module is placed in the cloud decryption module on the client, the data security can be effectively guaranteed, the public key is sent to the cloud for encryption, and the data is read and then placed on the client for decryption. However, this will increase the burden on the client, the client reads data at a lower speed, and the decryption process is opaque to the user.

For this purpose, a new RSA-based one-time-one-crypto encryption strategy has the following main objectives:

- Encryption and decryption are not performed on the client, and the entire process is transparent to the user.
- Encryption and decryption are implemented without using a cloud computing capability without increasing the burden on the client.

To ensure the security of the key, under the assumption that the network and server environment are not trusted, Although the secret is intercepted, records can't be accesses.

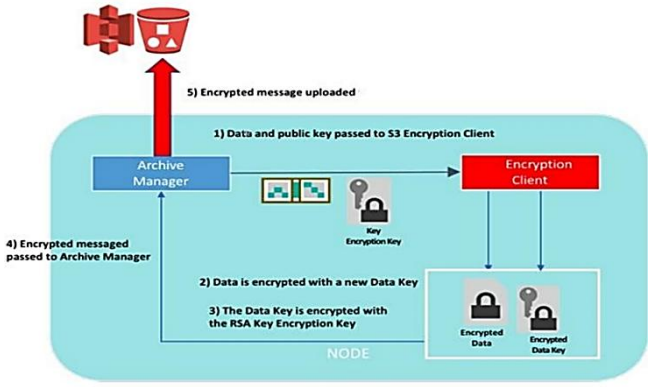

Fig. 3. Flow of RSA-based one-time encryption strategy.

In this encryption strategy, when a user stores data for the first time, a pair of public and private keys are generated in a separate key management module, and the data and public key are sent to the cloud encrypted storage at the same time. After that, every time you need to read the data, a new pair of RSA keys is generated, the New public key and the vintage non-public keys are sent to the cloud, and the new non-public key is saved in the key control module. The facts is decrypted with the old private key within the cloud and dispatched to the customer, and the statistics is encrypted again with the brand new public key. In this way, even supposing the antique non-public secret's intercepted, the records can't be received, due to the fact the information has been encrypted through the new public key, and the brand new personal key that may examine it has no longer been sent to the cloud. The encryption process is shown in Fig. 3.

This encryption strategy can be illustrated with an image example: The customer has a safe remotely. Whenever he comes to the safe to pick up things, the customer brings a new lock with the original safe and a new lock, and opens with the original key. The safe was taken out and locked with a new lock, and the new key was kept at home. In this way, even if the original key is maliciously copied, the new lock cannot be opened.

3) Key Management

In cloud data storage, how to manage key management for encrypting and decrypting data is a big problem. Key management needs to solve the following problems:

First, key management and data storage need to be performed separately. Key management and data storage cannot be put together, otherwise data will be lost if the key is stolen. Second, the key must be shared within a certain range, which is convenient for data synchronization between multiple terminals and for users in the same work group to share data. Therefore, the key cannot be stored on the client; otherwise, the user cannot use the key between multiple devices.

To this end, this solution stores the key in a separate key management module, and a field in each file or database corresponds to a separate key. When the user needs to read the data, he connects to the key management module, obtains the corresponding key according to his own authority, and then reads the data from the cloud platform [9].

4) Data Awareness

In the cloud environment, when someone operates on cloud data, the user should be able to perceive that the user's private data storage, use, modification, and deletion operations in the cloud can be perceived by the user. This requires the cloud to be able to record all access to cloud user data. At the same time, in some specific cases, operations on cloud data require additional identity authentication, such as allowing users to enter independent data read passwords. Through these methods, when someone operates on the cloud data, the user can know immediately, so as to determine whether someone is trying to steal data. In addition, in order to prevent data in the cloud from being tampered with, the cloud should also provide a file hash value comparison service that records the hash value of the cloud file at a certain time and compares it when the user needs it. If the comparison is unsuccessful, then This means that data in the cloud has been tampered with.

5) Data Sharing

In many cases, data in the cloud needs to be shared. A user may want to use cloud services to synchronize his photos on his mobile phone and computer. Enterprise users may need to share some data among colleagues and other activities. This makes data storage under cloud services both confidential and open, and requires a comprehensive permission management system, with data owners opening data access permissions for other users. At the same time, the user authentication method should be based on passwords and digital certificates. Key files cannot be stored on the client. Users should be allowed to access the cloud through unauthenticated devices. Therefore, special modules are needed to control user access to achieve trusted data sharing.

In shared data management, the following permissions should be set:

- *Fully open and readable:* All users can read this data, but cannot modify the data.
- *Fully open and readable:* all users can read and modify this data.
- *Partially open and readable:* Authorized users can read this data, but cannot modify it.
- *Partially open and readable:* Some authorized users can read and modify this data.
- *Not open:* Only the data owner can read and modify the data.

6) Accident Liability Determination

In the process of using cloud services, you should also pay attention to the preservation of corresponding electronic evidence and records. When data loss, data theft and other accidents occur, relevant personnel can be held accountable through corresponding records to discover security vulnerabilities. To this end, the cloud itself needs to have a logging function to record every operation on cloud data. Under the traditional cloud platform, data operation records are only performed in the cloud, which is not conducive to electronic evidence collection and accountability after a problem occurs. To this end, an independent module should be designed. When users access data in the cloud, they also leave operation records in this module. With two sets of log records, comparison and analysis can be performed to facilitate accountability.

B. Solutions based on trusted third parties

In areas such as e-commerce, the concept of trusted third parties has long been widely used. In the context of today's cloud computing, many users show distrust of cloud service providers, but have related needs to use the services they provide. Due to the special architecture of the cloud service, the power of the cloud service provider is too large and too concentrated, giving users a sense of instinctual distrust. In this case, the concept of a trusted third party is introduced, and part of the cloud's work is undertaken through a trusted third-party platform, weakening the cloud service provider's authority, and through a special working mechanism, it has a certain supervisory role for the cloud service administrator. At the same time, the risks are shared, and there will be no data leakage due to the breach of the cloud platform [10-12].

The trusted third-party platform under cloud services mainly provides the following functions:

- *Key management and data encryption services:* When users need to upload data to the cloud, they can manage the keys or encrypted data through a accesses third-party platform. The data in cloud is only encrypted data. Three parties obtain the key, and even the cloud administrator cannot steal user data. The only trusted third-party platform is the data key. If the encrypted data is not obtained from the cloud platform, the user data cannot be obtained even if the key is obtained. If someone wants to steal user data, they must control the cloud and a third-party platform at the same time. In the actual process, it is less likely that both will be breached at the same time.

- *Data sharing and rights management services:* In some cases, users need to share their data with others. Since trusted third parties manage the keys of all user data, they can be issued to users through rights management. Users with access rights to controllable sharing of secret data.

At the same time, with the cooperation of trusted third parties and the cloud, it can also provide the following functions:

- *Data awareness and controllable services*: The user's access to cloud data will leave records on both the third-party platform and the cloud, making the data more controllable.
- *Electronic evidence preservation and accident responsibility determination services:* All users access cloud data through the entrance of trusted third parties, so all access records of users will be recorded on trusted third-party platforms. At the same time, the cloud will also use the server's log records to directly access data records from the cloud platform distributed system. Users can regularly compare the two records to discover possible attempts to steal data. Third-party and cloud log records can be mutually verified and mutually monitored to prevent any of them from stealing data.

1) Trusted Third Party Platform Operation Model

There are two main modes of operation of trusted third-party platforms, as shown in Fig. 4. For individual users and small businesses, powerful third-party Internet companies can provide specialized cloud platform third-party services. Like third-party payment platforms such as phonepe, end users do not even need to pay any service fees for third-party services, because cloud service providers will bear trusted third-party service fees to attract users.

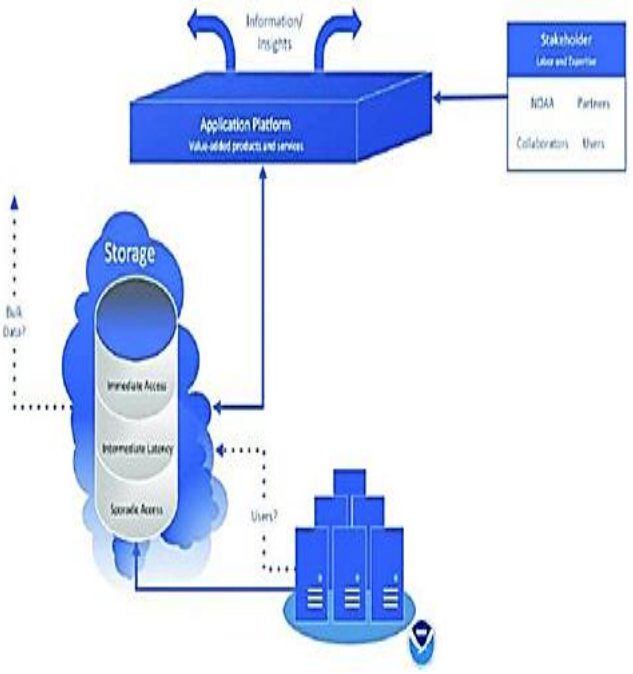

Fig. 4. Cloud platform operation model based on trusted third parties

For large enterprises and government agencies, if they require higher confidentiality or want to better control their own data, they can also build a third-party platform by themselves, put it in the corporate firewall, and use stricter management. The system and more perfect technical guarantees provide comprehensive protection.

2) Advantages of Trusted Third-Party Cloud Platform

A cloud platform based on a trusted third party has the following advantages:

- A trusted third-party platform is built on the basis of public clouds. There are sufficient cloud computing resources available for use, and there are very comprehensive security measures. You can enjoy the massive resources and high availability and scalability of public clouds. At the same time, it is as secure as a private cloud.
- The cost of building a trusted third-party platform is low and easy to promote. For service providers that provide trusted third-party services, the construction cost is low, the market demand is large, and there is huge market space. For large enterprises and government agencies who want to build their own third-party platforms, the cost of building a third-party platform is much lower than the cost of building a private cloud, but they can get the same security and more cloud resources as a private cloud.
- As far as the existing cloud computing architecture is concerned, the introduction of a trusted third-party platform has not made much changes to the existing cloud architecture, but just added an intermediary between the existing client and the cloud. This means that when a trusted third-party platform is deployed, there is no need to make excessive changes to the existing cloud architecture system, the cost of technical transformation is low, and the deployment cost is reduced.
- For end users, various security measures of trusted third parties are transparent. Although a series of measures such as data encryption have been adopted, users do not need to change the original usage habits. Advantages such as multi-terminal synchronization and data sharing still exist.

C. Cloud platform system architecture based on trusted third parties

Based totally on relied on events as shown in Fig. 5, a trusted celebration cloud platform system includes a consumer, a trusted 1/3-party platform, and the cloud. Among them, the consumer only performs the send request and upload / download information operations, and does now not carry out other calculations. Therefore, the purchaser does now not want to put in unique software program. The third-birthday party platform is a server with a database this is answerable for accepting purchaser requests, storing person statistics, coping with keys, and recording consumer operations on information. The cloud is responsible for storing encrypted data, and also stores user information, and records user operations on the data from the cloud.

In terms of data encryption, this solution provides two sets of solutions: the first solution is to use AES algorithm to encrypt the data on the third-party platform; the second solution is to use the one-time one-time encryption RSA algorithm to encrypt the data in the cloud. In use, users can choose the corresponding algorithm according to their needs and actual conditions.

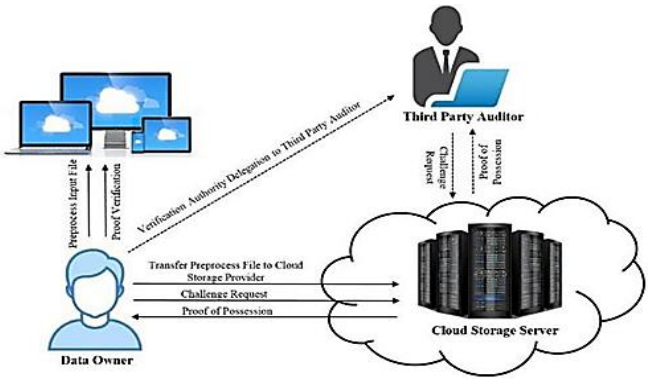

Fig. 5. Cloud platform system architecture based on trusted third parties.

D. Trusted Third Party Platform Workflow

1) Upload data process

When uploading data, the client first establishes a connection with a third-party platform. The third-party platform verifies the identity of the user. If the user uploads brand-new data, a corresponding record is added to the database. If the user wants to modify the existing data, check whether the user has permission to modify the data. If both the user authority authentication and the identity authentication are passed, the next phase is entered. If you use an AES encryption policy based on a third-party platform, a random 128-bit Advance Encryption Standard key will be automatically generated on the third-party platform. After the data is encrypted by the key, the key is stored in the database of the third-party platform. The data is sent to the cloud, which is stored after receiving the data [13]. If you use the cloud-based Rivest–Shamir–Adleman one-time encryption policy, a random pair of 1024-bit Rivest–Shamir–Adleman keys will be automatically generated on the third-party platform, and then the private key will be stored in the database, and the public key will be returned to the client, and the client will accept The public key is sent to the cloud together with the data, and the cloud encrypts the data with the public key passed [14,15].

2) Download data process

When downloading data, the client will first establish a connection with a third-party platform, and the third-party platform will verify the identity of the user and check the user permissions. If the user has read access to the requested data, then proceed to the next stage. If an Advanced Encryption Standard encryption policy based on a third-party platform is used, the third-party platform will read the key corresponding to the data, then obtain the encrypted data from the cloud, use the data key to decryption the data and send it to the client. If you use the cloud-based Rivest–Shamir–Adleman one-time encryption policy, the third-party platform will read the private key corresponding to the data, and then generate a new pair of Rivest–Shamir–Adleman keys, and store the new private key in the database instead of the original private key. Send the new public key and the original private key to the cloud. After receiving the key in the cloud, it decrypts the data with the original private key and sends the decrypted data to the client, and then re-encrypts the data with the new public key.

IV. PROPOSED SCHEME ADVANTAGES

With the increasing application of cloud computing, the security of data storage in the cloud environment will definitely receive more attention. This solution proposes the concept of a trusted third party in cloud data storage, and integrates the application of a trusted third-party platform into each link of cloud storage. Therefore, some new ideas and new methods for solving the security problems of public cloud data are proposed. Enhanced cloud data in all aspects of Storage security.

Traditional cloud data sharing often uses the "share link" or password method. This sharing mode is not highly controllable. If the share link or password is leaked, data may be obtained by users who do not want to share it It is impossible to know who has obtained the data. Through third-party platforms for identity authentication and rights management, allowing data to be shared in a controlled manner, data owners can conveniently add and delete shared users, allowing data to be shared within a controlled range without leaking to others.

Traditional key storage generally uses either a client or a server. But both methods have drawbacks. There is a server with the data. If the data is stolen, the key will be lost, and the data encryption will lose its meaning. If there is a client, data sharing and multi-terminal synchronization will be limited, users need to synchronize the update key when acquiring data on different terminals, and it will be very inconvenient to synchronize data on mobile terminals. The use of a third-party platform to manage keys will solve this problem very well. Through the aforementioned permission control and identification, multi-user, multi-platform, and multi-terminal key sharing can be easily achieved, thereby solving the key problem. At the same time, the key and data are not stored on the same platform, which also solves the security problem.

Traditional encryption strategies often use symmetric keys, which are not highly secure and the keys may be intercepted. The RSA-based one-time encryption strategy applies the "one-time one-pass" strategy to cloud data storage to ensure the security of the key, and the data cannot be read even if the key is intercepted. Leverage the powerful computing resources in the cloud to make up for the low encryption and decryption speed of the RSA asymmetric encryption algorithm.

In traditional cloud data storage, data perception and controllability are not high. Even if someone secretly manipulates the data, users cannot know that this solution records data on the third-party platform and the cloud at the same time. Compare and provide third-party credentials to prevent someone from illegally manipulating data, and to prevent files from being tampered with by hash check. At the same time, evidence is provided after a data theft and tampering event does occur for liability identification and prosecution. At present, although there are many solutions for public cloud data security in the market, they all have their own defects. Users have great needs for these functions. Introduce the concept of a trusted third-party platform to innovate traditional cloud operations and architecture models.

As an independent entity, the third-party platform can be operated by an Internet company, or it can be built and managed by an enterprise. In addition to public and private clouds, a new solution is provided.

V. CONCLUSION

With the increasing application of cloud computing, the security of data storage in the cloud environment will definitely receive more attention. This solution proposes the concept of a trusted third party in This solution has the advantages of massive resources of the public cloud, low cost, easy deployment and high expansion, and high availability. It also has the characteristics of private cloud security, privacy, and controllability. In addition, this solution is based on the public cloud, which solves the current data security problem of the public cloud, so that enterprise users do not have to invest a lot of money to build a private cloud, and small and medium-sized enterprises and individual users who cannot build a private cloud can also enjoy it on the public cloud platform. To private cloud security. This solution does not need to make much changes to the existing cloud platform architecture, low construction costs, short deployment time, and large market demand. Therefore, this solution has a good market application prospect.

REFERENCES

1. A. Abbas, K. Bilal, L. Zhang, S.U. Khan, “A cloud based health insurance plan recommendation system: a user centered approach”, Future Gener. Comput. Syst. (2014)
2. P. Mell, T. Grance, “The NIST definition of cloud computing”, NIST Special Publ. 800 (145) (2011) 7.
3. Che, Y. Duan, T. Zhang, J. Fan, “Study on the security models and strategies of cloud computing”, Proc. Eng. 23 (2011) 586–593.
4. M. Iorga, S. Chokhani, R. Chandramouli, “Cryptographic key management issues and challenges in cloud services, in: Secure Cloud Computing”, Springer, New York, 2014, pp. 1–30.
5. C. Wang, Q. Wang, K. Ren, N. Cao, W. Lou, “Toward secure and dependable storage services in cloud computing”, IEEE Trans. Services Comput. 5 (2) (2012) 220–232.
6. M. Balduzzi, J. Zaddach, D. Balzarotti, E. Kirda, S. Loureiro, “A security analysis of amazon’s elastic compute cloud service”, Proceedings of the 27th Annual ACM Symposium on Applied Computing, 2012, pp. 1427–1434.
7. 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.
8. Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing", Future Generation computer systems 28.6 (2012): 833-851.
9. A. Andrieux, K. Czajkowski, A. Dan, K. Keahey, H. Ludwig, T. Nakata, J. Pruyne, J. Rofrano, S. Tuecke, M. Xu, Web services agreement specification.
10. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, A. Ghalsasi, “Cloud computing the business perspective”, Decis. Support Syst. 51 (1) (2011) 176–189.
11. Hay. B, Nance. K, Bishop. M, “Storm clouds rising: security challenges for IaaS cloud computing”, in: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011, pp. 1–7.
12. Wei. L,Zhu. H,Cao. Z, Dong. X, Jia. W, Chen. Y, Vasilakos. A.V., “Security and privacy for storage and computation in cloud computing”, Inform. Sci. 258 (2014) 371–386.
13. Alowolodu O.D, Alese B.K, Adetunmbi A.O, Adewale O.S, Ogundele O.S, “Elliptic curve cryptography for securing cloud computing applications”, Int. J.Comput. Appl. 66 (2013).
14. Aslam. M, Gehrmann .C, Bjorkman M., “Security and trust preserving VM migrations in public clouds”, IEEE 11th International Conference on Trust,Security and Privacy in Computing and Communications (TrustCom), 2012, pp. 869–876.
15. Tang. Y, P.P. Lee, J.C.S. Lui, R. Perlman, “Secure overlay cloud storage with access control and assured deletion”, IEEE Trans. Dependable Secure Comput.9 (6) (2012) 903–916.

AUTHORS PROFILE

G. Nagi Reddy received his Master’s Degree in Computer Science and Engineering from Annamalai University, Tamil Nadu. He is currently an Assistant Professor in the Department of Computer Science and Engineering at Mahatma Gandhi Institute of Technology, Hyderabad. He has 13 years of teaching experience. He has 5 publications in international journals and conferences. His research areas include data mining, cloud computing, big data and data security.

P. Satya Shekar Varma received his Master’s Degree in Computer Science from Jawaharlal Nehru Technological University, Hyderabad. He is currently an Assistant Professor in the Department of Computer Science and Engineering at Mahatma Gandhi Institute of Technology, Hyderabad. He has 13 years of teaching experience. He has 14 publications in international journals and conferences. His research areas include data mining, cloud computing, big data and data security.