International Journal of Engineering, Management and Humanities (IJEMH)
Volume 5, Issue 3, May.-June, 2024 pp: 186-193 ISSN: 2584-2145
www.ijemh.com

A Method of Secure Access to Cloud Computing Data Based on Zero Trust

[1.]Wang Haipei, [2.] Tadiwa Elisha Nyamasvisva

[1]*Ph.D. student*, *Infrastructure University Kuala Lumpur,* Selangor Darul Ehsan, Malaysia

[2]*Dr., Infrastructure University Kuala Lumpur,* Selangor Darul Ehsan, Malaysia

Corresponding Author: Wang Haipei

Date of Submission: 12-06-2024 Date of Acceptance: 24-06-2024

ABSTRACT: Because of its high availability and elastic characteristics, cloud computing data storage will cause horizontal mobile attacks on cloud computing data, unauthorized access of system users, user data leakage and other security risks. Based on NIST zero trust architecture and extending software-defined boundary architecture, this paper proposes a zero trust cloud data storage security model combining SDP gateway and storage encryption gateway, and realizes active defense of cloud computing stored data by controlling access fine-grained permissions based on zero-trust identity agent encryption.

KEY WORDS: Zero trust, Software-defined boundary, Cloud computing,Data storage, Access control

I. INTRODUCTION

[1] With the development and deep integration of new technologies such as mobile Internet, Internet of Things, artificial intelligence, big data and cloud computing, more and more enterprises are realizing the digital and intelligent transformation of their business by going to the cloud. After enterprises go to the cloud, some new security risks will emerge due to the centralization and sharing of data. For example, cloud resources are flexibly configured in resource pool mode. Administrators can manage and allocate resources. Different users may access the same resource or the same user may access multiple resources. As a result, static configuration of access control policies in cloud scenarios is difficult. At the same time, the cloud service itself also has some security risks, including the risk of access permission, boundary risk, invisible internal traffic, and data isolation risk. When enterprise users use the Internet or private networks to access cloud services, data security and access behavior compliance and legality cannot be guaranteed. Traffic interaction within the cloud is invisible, and internal traffic changes and security threats cannot be detected, and threats cannot be controlled. Once hackers enter the private cloud, this openness facilitates the horizontal expansion of attacks . However, traditional security protection methods cannot effectively solve the above cloud security risks, so it is necessary to design a more ideal security solution.

Some cloud manufacturers have also launched security products and components such as cloud firewall, fortress machine, vulnerability scanning, DDoS protection, etc. These security products or components do play a role in security protection on some levels. However, there is still a lack of overall security planning, and various security devices and components fail to form a unified linkage, making it difficult to build a comprehensive security protection system behind the cloud. Therefore, combining with the security architecture of zero-trust network, this paper proposes a zero-trust based cloud computing data access model. According to the characteristics of cloud services and cloud storage data, the control plane access control model and trust transfer framework are refined, cloud data storage resource management and cloud storage data access security design are strengthened, and the security mechanism of cloud storage data access and encryption based on zero trust is proposed, so as to solve the security problem of cloud data access and storage.

II. RELATED WORK AND PROBLEMS

The concept of zero trust was first proposed by JohnKindervag of ForresterResearch. The core idea is "Never trust, always verify". SDP and MSG in zero-trust architecture are ideal solutions to North-South and east-west traffic control problems, respectively.

2.1 Zero-trust architecture

[2] Zero trust architecture is an architecture framework based on the concept of zero trust. It integrates access agents, zero-trust network planes, and service resources to protect the secure access between users and business data. The initial focus is

on limiting resources to those who need access and granting only the minimum access required to perform the task. NIST gives the core components of a zero-trust architecture, as illustrated in Figure 1.

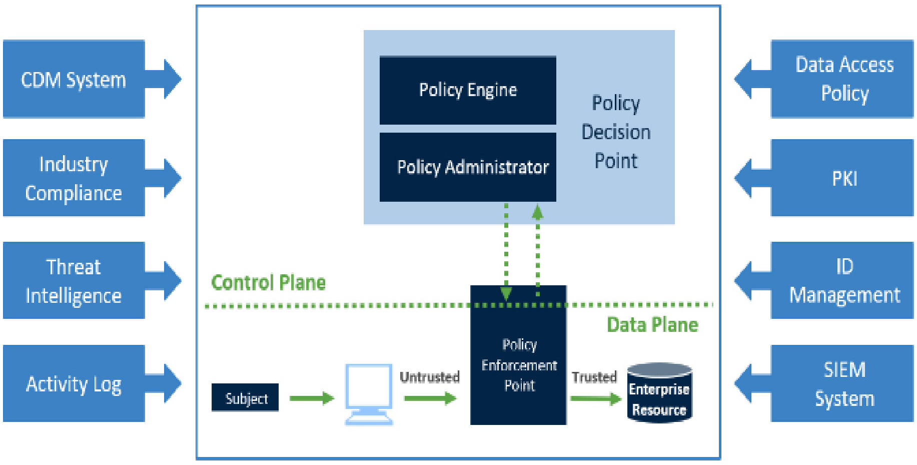

Figure 1 NIST Zero Trust architecture

2.2 Software-defined Boundary SDP

Software-defined Boundary (SDP) is a next-generation secure access solution based on a zero-trust architecture. SDP mainly includes SDP client, SDP controller, SDP gateway, but also includes single-packet authorization, dynamic firewall, device verification and so on. The SDP client runs on the end user's device and is used to communicate with the SDP controller to request a connection and send data information to the controller. The SDP client typically initiates an access request to the SDP controller in the form of a single-packet authorization. The SDP controller verifies the single-packet information sent by the SDP client. If the authentication succeeds, the SDP returns the corresponding policy information and ACL to the SDP client. The attacker cannot see the target resource, so various security risks are effectively avoided. SDP is considered to be the best implementation of the zero-trust concept. It adopts a triangular architecture to separate control channels and data channels to achieve secure access control of services. Therefore, SDP is suitable for remote office, application cloud, multi-party authorization and other business scenarios. Its technical architecture is shown in Figure 2.

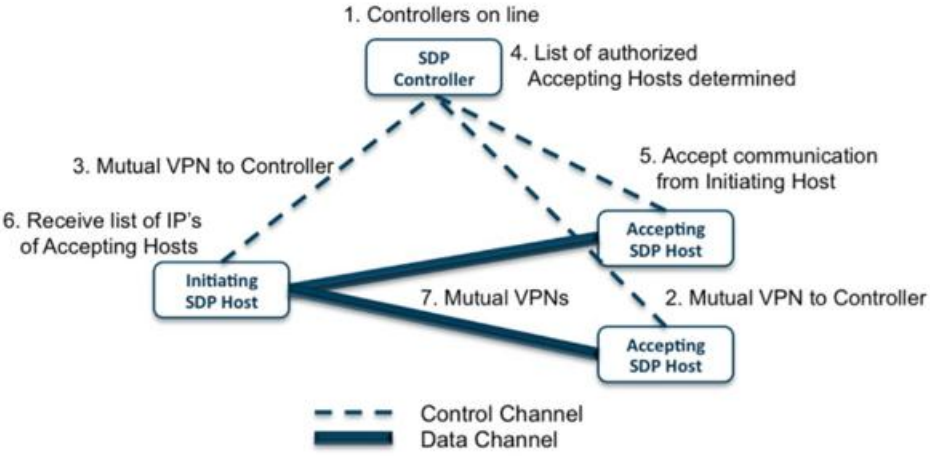
1. Controllers on line
SDP Controller
4. List of authorized Accepting Hosts determined
3. Mutual VPN to Controller
5. Accept communication from Initiating Host
6. Receive list of IP's of Accepting Hosts
Accepting SDP Host
Initiating SDP Host
7. Mutual VPNs
2. Mutual VPN to Controller
Accepting SDP Host
Control Channel
Data Channel

Figure 2 SDP architecture and workflow

[3] In addition to verifying SDP clients, the SDP controller also has the functions of situation awareness, risk management, and traffic audit. By default, the SDP gateway denies all access requests. After the client passes the authentication and the SDP controller delivers corresponding credentials and

policies, the SDP gateway connects to the SDP client and monitors the SDP client in real time. The biggest advantage of SDP is that it uses single-packet authorization to make the SDP network invisible, which minimizes the network attack surface and greatly reduces network security risks. SDP can hide all resources, illegal users cannot access resources, and legitimate users access traffic is transmitted through encryption. Active defense concepts such as continuous authentication and fine-grained access control can effectively solve the security problems in enterprise business development, and it is an effective way to solve the security protection problems of north-south traffic [5].

2.3 Encryption Algorithm

[5] [6] The commonly used data encryption algorithms are bilinear mapping, pseudo-random function and symmetric cryptosystem.

Definition 1(Bilinear mapping**)** lets G and G_T be a finite cyclic group of two primes p of order, and g be any generator of the group G. If the mapping $e{:}G\times G\rightarrow G_T$ satisfies :(1) Bilinear, i.e., for any a,b$Z\in_p$, there is $e(g^{ab}, g)=e(g, g)^{ab}$; (2) non-degenerate,$e(G,G) \neq 1$. Then e is said to be a (symmetric) bilinear map on (G_T,G).

Definition 2(DBDH hypothesis) Given a five-element $(g,g^a,g^b,g^c,T) \in G^4\times G_T$(where a,b,c ∈ Z_p is chosen at random), it is difficult to determine whether $T= e(g,g_T)^{abc}$ or a random element in G.

Definition 3(pseudorandom function**)** For any $j \in \{0,1\}^*$ and $k_{prf}\leftarrow K_{prf}$, $f{:}\{0,1\}^*\times K_{prf}\rightarrow Zp$, is a pseudorandom function if the result of a mapping between $fk_{prf}(j)$ and a true random function is computationally indistinguishable.

Definition 4(symmetric encryption**)** A symmetric encryption algorithm usually consists of an encryption algorithm E and a decryption algorithm D and satisfies $D(k,E\ (k,m))=m$. It should be semantically secure under selection-plaintext attacks.

2.4 This article solves the security problem of cloud data storage

This paper designs the trust preservation of any access subject, authentication before access, authentication after access data, and gives a dynamic encryption model of cloud storage based on zero trust. Analysis of the existing cloud storage data encryption to zero trust support, divided into two aspects. First, architecture design, computing nodes, storage nodes call virtual password card mode, can not achieve authentication before connection security, does not meet the security requirements of zero-trust architecture, based on storage encryption gateway mode, can achieve authentication before connection storage service security. The second is control plane access control, which realizes user identity management and verification, but does not realize the association between user identity and data encryption and decryption, and there is the risk of unauthorized access to user data by system users.

III. A CLOUD COMPUTING DATA ACCESS MODEL BASED ON ZERO TRUST

Based on NIST's zero trust model, the cloud storage encryption model adopts the trusted policy execution mode of the two gateways of "Trusted Connection Policy Execution Gateway (SDP Gateway)" and "Stored Data Access Policy Execution Gateway (Storage Encryption gateway)", as shown in Figure 3.

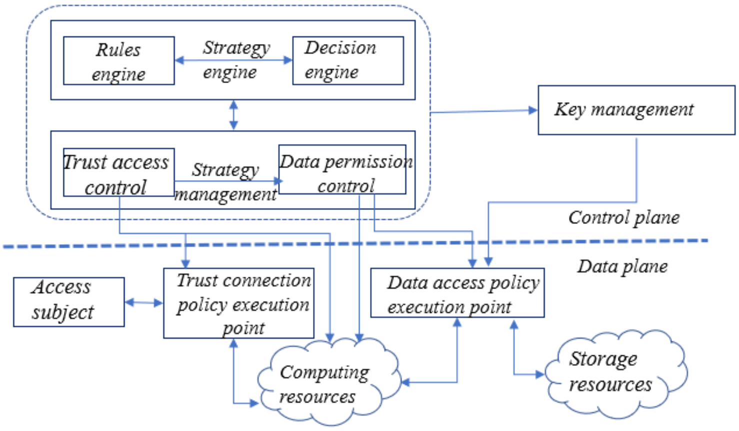

FIG. 3 Cloud data encryption model based on zero trust

(1) Separation of control plane and data plane

[4] The main function of the control plane is to build a policy controller through policy management and policy engine. The policy controller sends the policy to the execution point. The data plane consists of two policy execution points, the trust connection policy execution point and the storage data access policy execution point. The policy execution point performs security access, resource authorization management, data access (such as data backup), and data operations (read and write) based on the policy results. The control plane and data plane can be divided using different communication protocols and network topologies, and are virtualized and isolated in the system to realize logical isolation of the control plane and data plane.

(2) Control plane policy management model

Consistent with the zero trust model, the control plane includes a policy engine and a policy management component. Adapting to the complex system structure of cloud computing, policy management is divided into trust and access control model and data storage permission control model, which deal with cloud access control and cloud storage data access control respectively. Through the identity management, role and permission management, behavior and state dynamic analysis, rule engine and decision engine related to policy management, the trust and access control sub-model is built to obtain the trusted agent accessing the cloud computing node; Through the management of resource identification, resource attributes and operation permissions, as well as the corresponding rules and decision engine, the storage data access permission control sub-model is constructed to achieve the management, access and operation of the trusted subject to the specific attribute resources. The control plane adds storage key management based on access control. Through the access control and key delivery of the storage key, only authorized users have the key, and then read the stored data through key encryption and decryption. For system users who perform system-level operations in the cloud platform, such as automatic resource backup by the system, they only need to back up the secret state data, and use the access policy control of key management to avoid obtaining the user's storage key through system-level operations, thus failing to decrypt user data and avoiding the risk of system super users.

(3) Data surface policy execution

The trusted connection policy execution point is the first policy execution point for any user to access cloud resources. As a computing service agent, it can connect to the cloud computing node after obtaining the authentication of the trusted principal. The storage data access policy execution point is the second policy execution point for a user to access cloud storage resources. As a data storage service agent, on the one hand, it adopts the gateway mode to isolate computing services and user access. On the other hand, it ensures that only authentication and authorization entities can access cloud storage data resources, and only legitimate and authorized users/applications can decrypt the stored data.

2) Implementation architecture

Control surface policy management belongs to the cloud management platform. SDP gateway and storage encryption gateway are configured on the data plane respectively. Security context is associated between the gateways through policy management on the control plane, and the architecture is shown in Figure 4. SDP gateway is the agent for accessing the computing service of the main body, and also the execution point of the trusted connection policy for any user to access cloud resources. According to the access control rule set and constraint conditions constructed by the control plane for the identity management, user attributes, resource attributes and other relations of the access subject, as well as the dynamic evaluation of behavior and status, the SDP gateway cuts off or connects to the cloud computing node.

The storage encryption gateway is the agent for the subject to access the storage service, and also the execution point of the policy for any subject to access the cloud storage data. After the control plane obtains the trusted agent, it performs data operation authentication and obtains the correct storage encryption key. The access subject uses the storage encryption gateway to judge the data storage access policy, operation trust, and input and output data encryption and decryption to operate cloud storage data.

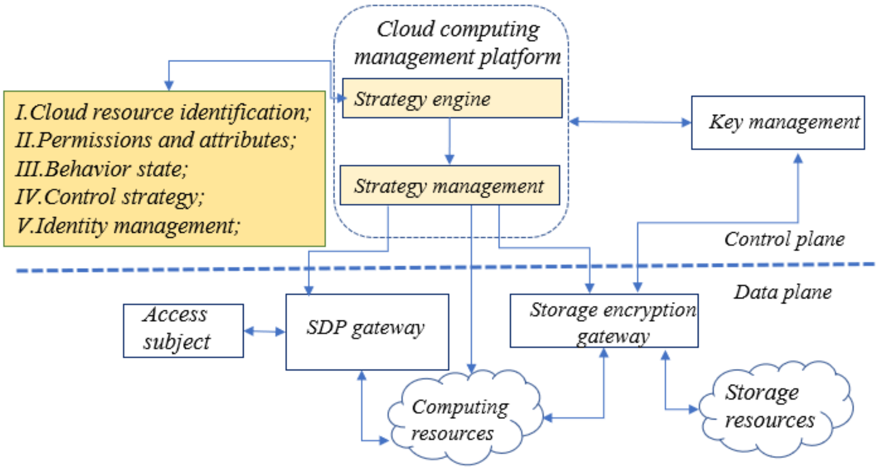

FIG. 4 Implementation architecture of cloud data encryption based on zero signal

3) Logical relationship

The cloud platform client initiates the operation request, and the access subject sends the management request to the cloud management platform control surface through the SDP gateway agent; The component of the control surface of the cloud management platform verifies the identity of the subject, and obtains the key management service by the trusted subject through authentication and network access control policies (identity, validity time, attributes, constraints, rule sets, etc.). The process of the control plane is as follows: access principal request →SDP control plane client →SDP control plane service (access trusted policy management and policy decision) > Delivery policy decision to SDP gateway;

Access principal request → cloud platform SDP control plane client →SDP control plane service (access trusted policy management and policy decision)→ Data access permission control → key management → policy decision delivery to the storage gateway.

The data surface process is divided into two stages. The first stage is the key establishment stage, followed by the access subject request → key management (or SSL authentication) → trust connection gateway → storage key management → storage encryption gateway; The second stage is the data access stage, access subject request → trust connection gateway → cloud computing node data plane → storage encryption gateway → cloud storage server data plane.

3.2 Control plane Trust and access control model refinement

Control surface policy management includes trust and access control model and data storage permission control model, which provides policy management and decision-making methods for SDP gateway and storage encryption gateway, and realizes the association relationship between the two models of subject (user/administrator/program) through trusted principal verification and trusted authorization operation. Specific rules, according to the specific scenario design, to meet the rules.

The relationship between each part of access control, the establishment of the overall security model of access control is shown in Figure 5.

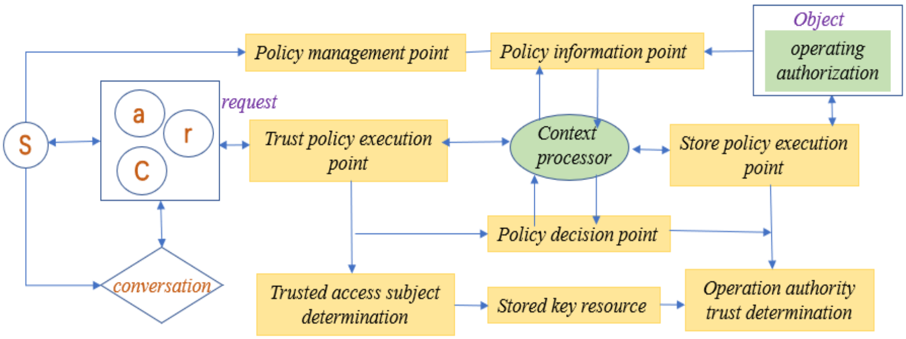

Figure 5 Zero trust access control model for cloud resources

1) Unified definition and identification

S: The main body of the access request is the initiator of the resource access, which can be a user, a program, a system administrator, etc. $S =\{<uID,a,r,z>\}$, where *uID* indicates the unique identifier of the subject; a is the subject's security level and other attributes; r is the task role of the subject classification; z indicates the state of the subject, and the initial state of z is 0, indicating that no access has occurred to the subject;

"Parameter Description Value": "resource", indicating the accessed object and its related properties, "parameter meaning" parameter meaning ". *sID* is the unique identifier of the resource. c identifies the category and source of the resource; g represents the attribute of the resource, such as security level, private or shared. z identifies the state of the resource. For example, in a cloud environment, identify computing resource pools (*VM CPU memory, virtual IP address, and assigned user*), storage resource pools (*logical volume ID, secret level, assigned user, and dedicated machine address*), and key service resource pools (*key number, key attribute, and physical address > of key resources*).

Op operation: defined as the specific access behavior to resources. Including but not limited to management (*configuration, query, modify, assign binding, migration, backup, etc.*) and use (*connect, disconnect, read and write (read only, write only), clear*) operations, each operation is defined with a unique ID.

Rule set SC and constraint Const: *SC={attribute, role, task, permission}; Const={time, access point, port, policy match}→z.*

TrS: Trusted access subject, $TrS=\{<S, Time, Trust, Sign>\}$, an entity whose signature is unforgeable by cryptographic functions and can be verified as legitimate by a third party. Time- time information, Trust- trust level, Sign- unforgeable signature.

2) Trust and access Control Framework

Trust and access control structure: *{S, O, Op, SC, Const}* constitutes the authorized access control structure and defines the access policy and the method of updating the access policy to obtain the target result. For example, administrator classification and permission rule set user classification and permission rule set; System automatic operation (migration, high security, etc.) class and permission rules set; Dynamic evaluation rule set, permission rule set constraint condition Const that changes with dynamic analysis evaluation result; The type classification of resource access by the resource operation Op

The goal result of trust and authorization access control is to obtain a trusted access subject :$TrS=\{S|S\rightarrow O$, *whose S satisfies authentication, policy set SC (permissions, properties), constraint Const (location, time, access point), etc.}.*

3) Data storage permission control framework

The request access subject has a certain state ($state =\{S\times O\times OP\}$), such as inactive state, blacklist state, etc. The collection of resources in the cloud also has certain states, such as initial state, used state, backed up state, exhausted state, deleted state, etc.

States express context and timing. An operation judged to be legal for a trusted agent in one state may be an operation that does not satisfy the rules or is illegal in another state.

Data store access *structure ={TrS, only computing resource, only key resource, only storage resource, only p, SC, Const, F}*;

TrOp trusted access main structure, when Time, permission and other rules and constraints are met, that is, the parameter *<O, Time, Trust, Sign>* is input, calculated through $TrS\rightarrow O$ $||TrS>O$ storage *key* $||TrS\rightarrow O$ storage policy const condition judgment, SC rule compliance judgment, etc. The objective function is the operation *TrOp ID*.

In order to meet the characteristics of diverse types and dynamic changes of access agents in cloud scenarios, state changes are added to the agents. The model is general and has the following security:

(1) Unified identification of the access subject, including the status attribute of the subject;

(2) Unique identification of resources, including the security level and status attributes of resources;

(3) Increase the judgment of *TrS* trusted access subjects, and only authentication and authorization subjects can access the cloud platform;

(4) Add $TrS>O$ computing $TrS\rightarrow O$ storage *key*$||TrS\rightarrow O$ storage operation permission *TrOp* judgment, and only authenticate and authorize principals to manage and configure cloud storage resources;

(5) Only authenticates and authorizes subjects to access data storage resources;

(6) Only authenticate authorized users to add/decrypt static storage data.

IV. ACCESS MAIN STORAGE KEY MANAGEMENT DESIGN AND SCHEME DESCRIPTION

In view of users' urgent demand for secure cloud storage and sharing of private data, this section presents a practical solution based on the idea of trust-based identity proxy encryption: the data owner encrypts the data to the cloud server, and when other users request access to the data, the proxy server uses the re-encryption key to convert the ciphertext into the ciphertext accessible to the data sharer, as shown in Figure 6.

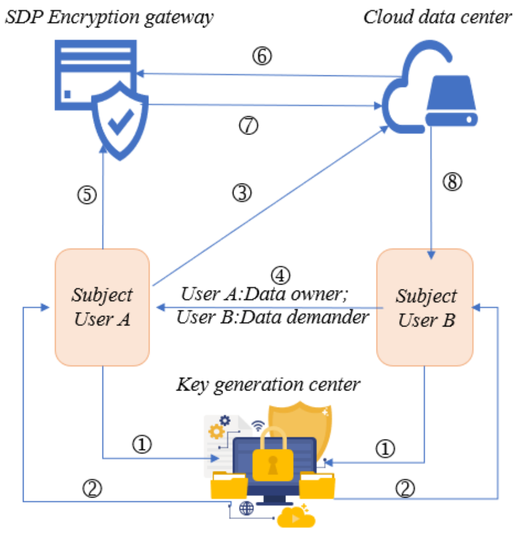

Figure 6 Access subject storage key management

①Identity authentication; ②Return private key skB and system parameter mpk; ③Upload encrypted data; ④Request access to data; ⑤Data key; ⑥Read data; ⑦Converted data; ⑧Access data

4.1 Access principal storage key management design

(1) System initialization algorithm $Setup(1^{\lambda})$: Input security parameter 1^{λ}, key generation center generates system main public key mpk and system main private key msk. The master public key is shared by all users in the system.

(2) Partial private key generation algorithm $PKGen(msk,id)$: Input the main private key msk and user id, and the key generation center calculates the partial private key sk_{id} corresponding to the user id.

(3) User encryption and decryption key generation algorithm $UKGen(mpk, sk_{id})$: input the main public key mpk of the system and part of the user's private key sk_{id}, and the user generates its own encryption key ek_{id} and decryption key dk_{id}.

(4) Encryption algorithm $Encrypt\ (ek_{id},id,\ j,m)$: Input the user's encryption key ek_{id}, user id, data m and its $ID\ j$, and the data owner encrypts the data and uploads the ciphertext $C_{j,id}$ to the cloud storage server.

(5)Proxy key generation algorithm $RKGen(sk_{id1}, j,id_1,id)$: User id_2, using the decryption key sk_{id1}, generates the re-encryption key $rk_j,id_1 \rightarrow id_2$ of data j and sends it to the proxy server.

(6)Re-encryption algorithm $ReEncrypt(rk_{j,ad1\rightarrow id2},C_{j,id})$:Input the re-encryption key $rk_{j,ad1\rightarrow id2}$, and ciphertext $C_{j,id1}$, and the proxy server converts the ciphertext of the data identified as j into the ciphertext C of the user id_2

(7) Decrypt algorithm $Decrypt(dk,C_{j,id})$: Input the user decryption key dk_{id} and ciphertext $C_{j,id}$, and recover the data information identified as j by the user id.

4.2 Scheme Description

(1) the system parameters, selection of bilinear mapping (G, G_T, e, G, p), hash function $H:\{0,l\}^* \rightarrow G$ and $H_1:\{0,1\}^* \rightarrow \{0,1\}^{128}$; Symmetric encryption algorithm (E,D). Then s∈Z is selected at random, and h= G.^{s} Finally, the main public key $mpk=(G,G_T, e,g,p,h,H,H_1,E,D)$ and the main private key $msk =(mpk,s)$ are returned.

(2) Partial private key $:KGC$ uses the main private key to calculate and return $sk_{id}= H(id)^s$.

(3) Encryption and decryption keys: User id selects the key $k \leftarrow_{prf} K$ of a pseudo-random function $f:\{0,l\}^* \times K_{prfprf} \rightarrow Z_p$ and returns $ek_{id} = (mpk,k_{prf})$ and $dk_{id}= (sk_{id},k_{prf})$.

(4) encryption: randomly selected r∈Z_p, and R∈

G_T, calculating $k_{AES} = H_1(R)$、$t = f_{kprf}(j)$ 、$c_0=E(k_{AES}, m)$ 、$C1= g^r$ *and* $c_2=R.\ e(g^s, H(id)^{rt})$.*Return* $C_{j,id}= (c_0,c_1,c_2)$.

(5) Reencryption key: Calculate the reencryption key $rk_{j,id1\rightarrow id2}$. And sent to the proxy server, and then calculate $K_{id1,,id2}= e\ (H\ (id)^s, H\ (id_2))$ *and* $t = f_{kprf}\ (j)$, and finally return to fairly $rk_{j,id1\rightarrow id2}= H\ (id_1)^{-st}\cdot H\ (K_{id1,id2})$.

(6) Re-encrypt ciphertext: Given the ciphertext $C_{j,id1}$, $=(c_0,c_1,c_2)$, the proxy server converts it into the ciphertext of the user id_2 as follows: Compute $c'2= c_2\cdot e(c_1,rk_j,id_1\rightarrow id_2)$ and return $C_{j,id2}= (c_0,c_2, c'_2)$.

(7) Decryption: The user uses the key dk_{id} to recover the data information identified as j in the following way:

① If C_j,id is the original ciphertext, that is, the ciphertext encrypted by the user id itself, then $t = f_{kprf}(j)$ is calculated first, then $R=C_2\cdot e(c_1,H(id)^{-st})$ and $k_{AES}=H_1(R)$ are calculated, and finally returned $m=D(k_{AES},c_0)$.

② if $C_{j,id}$ is a proxy server is changed after the ciphertext, is first calculated $K_{id,id'} = e\ (H\ (id)^s, H\ (id'))$, to calculate $R=c_2\cdot e(c_1,H(K_{id1,\ id2})^{-1})$ and $K_{AES} = H_1(R)$, and finally return to $m=D\ (K_{AES}, C_0)$.

V. CONCLUSION

By studying the existing zero-trust architecture and cloud data storage encryption technology, this paper proposes a zero-trust cloud storage encryption model based on SDP gateway and storage encryption gateway. On this basis, the overall security design of authentication, fine-grained access control and storage key management is enhanced. By increasing the judgment of trusted access subjects, only authentication and authorization subjects can access the cloud platform; *Add TrS→O computing||TrS→>O storage key ||TrS>O* storage multi-node, trust transfer, and operation right *TrOp* judgment, and only authentication and authorization entities can manage and configure cloud storage resources. Ensure that only authorized subjects are authenticated to access data storage resources. The dual computational authentication mechanism of key authentication and access principal authentication is designed for the storage encryption gateway to ensure that only authorized users have the key, and then add/decrypt the statically stored data. Expanding the "authentication before connection" security of zero-trust network into the cloud platform data storage security design of "authentication before resource management" and "authentication before data operation" is of great significance for realizing cloud data security.

REFERENCES

[1]. Cloud Security Technical Reference Architecture V1.O.(2021),Cybersecurity and Infrastructure Security Agency, August 2021.

[2]. Scott,R;Oliver,B; and Stu Mitchell.(2020),ZeroTrustArchitectue. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf, August 2020.

[3]. Paul,T; and Krithiga,G.(2021),Approaching Zero TrustSecurity with Oracle Cloud Infrastructure. https://www.oracle.com, 2021.8.

[4]. Meng,H; and Liu, J. (2023), Research on Data storage encryption model in cloud environment based on zero trust. Network Security Technology and Application, 62-68.

[5]. MELL. P,(2009),The NIST definition of cloud computing. National Institute of Standards and Tech-nology, 2009 does (6) : 50.

[6]. Wang,X;Fu,H; and Zhang,L.(2010) ,Advances in attribute-based access control. Acta Electronica Sinica, 2010,38 (7): 1660-1667.]

[7]. Hong,C;Zhang,M;andFeng,D.(2011),Efficient Dynamic Ciphertext Access control Method for Cloud Storage. Journal of Communications, 2011,32 (7):125-132.