SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I8P107

Volume 10 Issue 8, 68-77, August 2023

Original Article

A Concrete Construction Encryption Mechanism Based Spatio Temporal Analysis for Securing BigData Storage in Cloud

S. Vijayanand[1], C. Viji[2], S. Vijayalakshmi[3], G. Vennila[4], B. Prabhu Shankar[5], N. Rajkumar[6]

[1]*Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bangalore, Karnataka, India.*
[2,5,6]*Department of Computer Science & Engineering, Alliance College of Engineering and Design, Alliance University, Bangalore, Karnataka, India.*
[3]*Department of Computer Science & Engineering, CMR Institute of Technology, Bangalore, Karnataka, India.*
[4]*Department of AIML, School of Computing, Mohan Babu University, Tirupati, Andhra Pradesh, India.*

[1]*Corresponding Author : vijayanand.s@jainuniversity.ac.in*

Received: 11 June 2023 Revised: 15 July 2023 Accepted: 10 August 2023 Published: 31 August 2023

Abstract - *Cloud computing has regenerated how processing infrastructure is abstracted and used as a significant architecture for large-scale computation. In addition to the issues posed by Big Data storage, the rapid growth of cloud computing increases the complexity of data confidentiality, data security, and user access regulations, resulting in a loss of cloud service trustworthiness. The country and society rely heavily on its security. We introduce a new, improved NTRU cryptosystem that raises an alert whenever it detects quantum computing attacks to extract spatial and temporal features. A Spatio-temporal constrained Secure and Verifiable Attribute-Based Access Control Scheme (SSVAABAC) is proposed in this research. This method's primary purpose is to successfully update and check access policies to improve authorization flexibility, resource usage, and business timeliness. On the one hand, INTRU cryptosystem and Attribute Based Access Control (ABAC) Schemes are combined to improve the efficiency of security strength in cloud servers and provide efficient access policies enforced access decisions without adding any permission. It is easier to modify attributes than to change or define new roles in cloud servers by data owners, resulting in less computational overhead than traditional methods. On the other hand, the developed SSVA-ACS will support temporal and spatial constrained attributes to enable the user's accessibility of cypher text from CSs associated with the location and valid time interval. The effectiveness of decryption is successful if the Access policies and Spatio-temporal details of users satisfy data owners' detail. Thus, the proposed scheme fits the user secret key for the users specified in the location and time interval. As a result, a concrete structure implements the suggested technique by implementing an encryption device that associates a user's time-related privilege with the current access time. The final results show that the SVACS and ABAC are more effective than the SSVAACS.*

Keywords - *Adaptive NTRU cryptosystem, Attribute based access control, Big data, Cloud computing, Spatio temporal analysis, SVACS and ABAC.*

1. Introduction

Cloud computing and extensive data analyses are booming development in information technology growth in recent days [1, 2]. This provides customers with an affordable and knowledge-learning-based service to process the data in centralized computing progress. Due to the public accessibility of data in a centralized environment, security and privacy are challenging to create testable resources for the users. So confidence and trust is an essential fact for providing this service. To this concern, cloud storage is optimized for higher security from the server dependencies through service providers to protect the data [3].

Cloud users have various types of data stored in cloud storage. There is no optimality to access logical levels during security principles.

For example, personal data have sensitive information and patient biodata, so the difference in handling the structure of data dependencies is logically varied due to the importance of data [4-6]. So they decide on security and controls to provide role-based access control to own the data. This creates a server-level contract for accessing the authentication policy through Service Level Agreements (SLA) [7].

The cloud provider offers various services like computing, storage, load balancer, and network under the integrity nature of security, responsibility, scalability, availability etc. [6]. However, in most classes, their centralized environment gets affected by security issues because of anomalies. All the acceptability in the cloud is through service-level agreements [7]. During the Big data analysis, map reducing, learning sensitivity, and privacy terms are analyzed to identify anomalies and provide a secure environment through cryptographic approaches [8, 9].

CS requires Cloud cryptography [10], a type of encryption that protects data in the cloud. Several safeguards are being implemented in cloud cryptography to prevent data from being breached, hacked, or infected by malware [11, 12]. Access privileges are governed not only by qualities but also by environmental factors such as time and location.

In light of the concerns mentioned above about user access privilege, an enhanced NTRU cryptosystem has been proposed [13]. The NTRU cryptosystem is built on the Shortest Vector Problem (SVP) on a lattice, which allows it to be swift and resilient to significant calculating assaults. It has been demonstrated that it is faster than RSA [14, 15, 32]. NTRU is a lattice-based public-key cryptosystem that is patented and open source to encrypt and decrypt data.

ABAC [16] is created to secure data in various resources link, remote devices, and Information Technology resources by blocking unauthorized access and activities from accessing them while adhering to the organization's standard security policies.

Moreover, ABAC [17] is a variation of traditional role-based access control. Roles define prerogatives flexibly determined based on any attribute of the actor trying to insert or change data, any vital characteristic of the valid data to be used or modified, or any contextual data available throughout a transaction.

This paper proposes a Spatio-temporal constrained, Secure and Verifiable Attribute-Based Access Control Scheme (SSVA-ABACS). This scheme combines SVACS and the ABAC with temporal and spatial constrained attributes to enable the user's accessibility of cipher text from CSs associated with the location and valid time interval. This scheme will verify that user's access policies and Spatio-temporal information satisfies the data owner's details for the successful decryption process. As a result, the suggested approach is appropriate for users whose secret keys are defined in terms of location and time interval.

The created solution is initiated by implementing the encryption mechanism to improve the implementation of new systems that attains performance and privileges to accept the time. Section II contains the related works of this research. Section III defines INTRU-ABACS and SSVAABACS implementations-section IV results and evaluations. Section V concludes performance and future work.

2. Related Work

This section describes the author's principles and methods that work together in the big data cloud environment. The cloud builds for standard storage as a centralized service for a communication environment to secure a safe attribute-based access control approach in a mobile cloud environment [18, 32]. The impact of secure data is attained by encryption and decryption access by key policy attribute-based encryption to protect the data in cloud servers [19]; this makes secured access in the smart grid computing system.

In [20], the authors described the access control policy to access his data from a vast storage medium to control the access rights through a dynamic updating policy. An outsourced policy update technique for ABE systems was developed as part of this scheme.

[21] Based on data acquired from mobile crowdsourcing, proposed an efficient solution for a set of operations in extensive data analysis. In [22], the author developed an efficient access control scheme using the attribute encryption algorithm and minimal cover set techniques. A user binary tree was constructed to generate Cloud Encryption Key (CEK) and utilized a proxy to do the partial decryption process.

[23] For cloud computing environments, a scalable attribute-based access control mechanism was introduced. The technique expands CP-ABE in a hierarchical user structure to accomplish scalability and fine-grained access control at the same time. Furthermore, this method allows a group of users to share access privileges in order to address the role jointly.

[17] Proposed TSC-ABAC, a new temporal and spatial restricted access control method that might efficiently address time and location limitations in cloud computing. The proxy re-encryption technique would be used in a concrete implementation of this method to correlate a user's time-related permission with the current access time [24]. [25] Created a model based on a cryptographic conspiracy involving cryptographic control CP-ABE. The CP-ABE level with a constant size cypher was first validated and evaluated, with total ratings for this method.

[26] Proposed a hierarchical CP-ABE technique with a Linear Secret Sharing Scheme (LSSS) matrix as the access structure. The algorithm merged multiple hierarchical access control structures of data fly into a single LSSS matrix, encrypting the full cypher text. An Attribute-Based

Hierarchical data Access Control system (AHAC) was built in cloud computing based on the developed CP-ABE algorithm. An Attribute-Based Data Access Management Scheme for Sensor-Cloud (ABDM-SC) was presented to solve the difficulty of flexible and secure data sharing[27]. The cryptography enhancement creates an attribute access policy based on fine-grained access rights to verify the authenticity; the hash-proof primitive methods are intended to achieve security depending on user authentication. In [28], Proposed a CPABE scheme that is traceable, revocable, accountable, and key-escrow free (TRAK-CPABE). This solution supports white-box traceability and direct revocation. After publishing to a cloud server [29, 30], this procedure divides the original data.

[31] With compute outsourcing and collusion resistance, a decentralized and expressive Cipher text Policy - Attribute-Based Keyword Search (CP-ABKS) system was proposed. A novel data publish-subscribe method was created based on the suggested CP-ABKS to achieve secure and flexible data sharing among numerous users.

3. Proposed Methodology

The INTRU Cryptosystem and ABAC schemes employing SSVA-ABACS are briefly explained in this section. This proposed system optimized with the lattice behavioural approach depends on the Shortest Vector Problem (SVP) to attain high-security assessment to compute the evaluation.

Compared with RSA security standards, this achieves high performance with additional secret features. These NTRU cryptographic approaches create a secret sharing approach based on crucial verification features on distributing a multiparty secret sharing approach.

The reconstruction occurs during the security process on a random attribute-based access policy. ABAC is decided by comparing features connected with the subject, object, request processes, and, in some cases, environmental factors that specify the permissible operations for a particular set of inputs; by intent, a new secret sharing critical aggregation process makes secure access to protect the data in the cloud server. A concrete construction scheme implements the suggested technique by encrypting a user's depends on the session verification to provide access rights.

3.1. Adaptive NTRU Cryptosystem with Access Control Scheme

To attain a secure cryptosystem to improve the access control scheme using INTRU implemented to enhance the security in cloud servers. To attain the three-level integer parameter, which contains $(\mathrm{N}, \mathrm{p}, \mathrm{q})$ with greed polynomial integer coefficient (N-1) with four level set of supportive integers l_{sk}, l_g,l_φ, and l_m.

Let us consider the prime factor that p, and q are regressed to attain $\gcd(p; q) = 1$ and $q > p$. Also, the NTRU works on the principle of ring formation '$R = Z[X]\backslash(X^N - 1), l_{sk}, l_g, l_\varphi, \text{and} l_m$' which is defined as 'R' as selection explained in (Hu et al. 2017). The polynomial vector space is $sk \in l_{sk}$ is represented as, The polynomial degree of evaluation defined by access policy $T - 1$

$$pk(x) = ok_0 + \sum_{T+1}^{T-1} h_i x^i \tag{1}$$

$$sk = \sum_{i=0}^{N-1} sk_i x^i = [sk_0, sk_1, \ldots., sk_{N-1}] \tag{2}$$

The convolution multiplies the skand g polynomials in R based on (2) defined by * computation by a multiplicative factor

$$sk * g = pk \text{ with } b_k = \sum_{i=0}^{k} sk_i\, gk - i + \sum_{i=k+1}^{N-1} sk_i gN + k - i \tag{3}$$

3.1.1. Keygen Process

This process creates a secure transaction verification key using public pk and private keys sk; consider the Alice bob data access through communication by randomly choosing polynomials in two way $g \in l_g$and $sk \in l_{sk}$ based on the inverse transformation of the Private key $|q|$, and inverse $|p|$as denotes as repsctively formation sk_q and sk_p be represented as

$$sk_q * sk = 1(|q|) \text{ and } sk_p * sk = 1(modp) \tag{4}$$

Through the Euclidian distance, the property of sk to process the selected sk_qandsk_p. During the transmission, Bob attains their pk based on the public key using (4), referred as $\{p, q, pk\}$ be represented as

$$pk = sk_q * g(modq) \tag{5}$$

3.1.2. Data Encryption

Let us assume that the message m sends to bob request that data. But thy encryption takes place m to process into polynomial in l_m. For representing the polynomial representation randomly, point $\varphi \in l_\varphi$ to encrypt the data based on Bob's public key using (5) and encrypt the message E_m to bob is

$$E_m = p\varphi * pk + m(modq) \tag{6}$$

3.1.3. Data Decryption

To receive the Encrypted message E_m from Alice to Bob, to decrypt the data through private key sk to take inverse dependencies of critical message m mod p like sk_pvia (7) and (8).

$$a = e * sk(modq) \tag{7}$$

$$m = a * sk(modp) \quad (8)$$

The polynomial function F(x) is initiated to construct the T-1 to the degree of evaluation (9)

$$F(x) = s + \sum_{i=1}^{T-1} \mu_i x^i \quad (9)$$

These T users can reconstruct the secret $s = F(0)$ from $s_1 = F(x_1), \dots, st = F(x_t)$ by computing

$$s = F(0) = \sum_{i=1}^{T} (s_i \prod_{i \in [1,n], i \neq j} \frac{0 - x_j}{x_i - x_j}) \quad (10)$$

3.1.4. Instance 1

Let us consider $a_i \geq 0$, be represented by $a_i = \frac{q-1}{2}\gamma + c_i^{\gamma+1}$, as same $0 \leq c_i^{\gamma+1} < \frac{q}{2}$. Pointed in the following sub instances.

Sub-Instance 1-1

If $\gamma = 0$, $a_{i'} = a_i$, then set $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\Gamma)} = 0$.

Sub-Instance 1-2

If $\gamma \geq 1$, set $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = \frac{q-1}{2}\gamma + c_i^{\gamma+1}$ and $c_i^{\gamma+2} = \cdots = c_i^{(\Gamma)} = 0$ then $a_{i'} = a_i$ - $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = c_i^{\gamma+1}$.

3.1.5. Instance 2

If $a_i < 0$, be represented by $a_i = -\frac{q-1}{2}\gamma + c_i^{\gamma+1}$, as same $-\frac{q}{2} < c_i^{\gamma+1} < 0$ pointed in the following sub instances.

Sub-Instance 2-1

If $\gamma = 0$, $a_{i'} = a_i$, then set $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\Gamma)} = 0$.

Sub-Instance 2-2

If $\gamma \geq 1$, set $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = \frac{q-1}{2}\gamma + c_i^{\gamma+1}$ and $c_i^{\gamma+2} = \cdots = c_i^{(\Gamma)} = 0$ then $a_{i'} = a_i$ - $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = c_i^{\gamma+1}$

Optimized security is obtained based on integrating the reality of NTRU encryption to eliminate decryption failures by observing the content. The steps given below shoes the INTRU algorithm procedures.

Algorithm 1 INTRU decryption

Step 1: Input: Encrypted message t c, Key security sk, sk_p
Step 2: Output: original message m;
Step 3: Compute $sa = e * sk$ for decryption;
Step 4: $\mathbf{\Gamma}$ = max $\{|\max_{0 \leq i \leq N-1} \{a_i\}|, |\max_{0 \leq i \leq N-1} \{a_i\}|\}$
Step 5: $\boldsymbol{\tau} = \left\lfloor \frac{\Gamma}{q/2} \right\rfloor$;
Step 6: If $\tau = 0$
Step 7: $\boldsymbol{m} = a * sk_p(\text{modp})$
Step 8: Else
Step 9: For $0 \leq i \leq N-1$,
Step 10: Compute $\gamma = \left\lfloor \frac{|a_i|}{q/2} \right\rfloor$
Step 11: if $\gamma = 0$
Step 12: $a_i' = a_i$ and $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\Gamma)} = 0$
Step 13: ElseIf $a_i > 0$;
Step 14: $a_i' = a_i - \frac{q-1}{2}\gamma$
Step 15: $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = \frac{q-1}{2}$
Step 16: $c_i^{\gamma+1} = a_i'$
Step 17: $c_i^{\gamma+2} = \cdots = c_i^{(\Gamma)} = 0$;
Step 18: Else
Step 19: $a_i' = a_i - \frac{q-1}{2}\gamma$
Step 20: $c_i^{(1)} = c_i^{(2)} = c_i^{(3)} = \cdots . = c_i^{(\gamma)} = -\frac{q-1}{2}$
Step 21: $c_i^{\gamma+1} = a_i'$
Step 22: $c_i^{\gamma+2} = \cdots = c_i^{(\Gamma)} = 0$;
Step 23: Endif
Step 24: Endfor
Step 25: $m' = a' * sk_p + c^{(1)} * sk_p + \cdots + c^{(\tau)} * sk_p(\text{modp})$
Step 26: Output Plaintext m'

3.2. Attribute-Based Access Control Scheme for Policy Attainment

The integration of combined optimization policy using ABAC support verifiable access policies to make higher scalability at the NTRU system for accessing service optimality more securely. The policy be defined as,

$$ABAC_{Policy} = \{P_m | \, m \in [1, M], P_m \; is \; a \; policy\} \quad (11)$$

We defined the abacdf () function in ABAC, which accepts as parameters the requestor, service, resource, and environment properties. P n abacdf(), the evaluation function of policy P n, is defined as follows in equation (12)

$$P_n abacdf(Attr(Req,) \, Attr(Serv), Attr(Res) Attr(Env) = permit \; or \; deny \quad (12)$$

3.3. Stages in the Proposed Scheme of Spatio-Temporal Constrained Secure and VABAC

The outline contains of the subsequent five phases:

3.3.1. System Initialization

The data prepared to secure with public and private keys be generated by the data owner by NTRU cryptography optimization.

System Construction

Based on the time limits $t_{[t_a t_b]}$ the accessing more user, the owner creates a bub key for each user 'B' and creates the certificate signing of message m→s with specified location Loc, and encrypts the message.

Sub-Key Creation

Based on different integers $b_0, b_1, \dots, b_{T-1}$ the data owners generate the subkeys randomly at $'T'$ levels, where pubic keys $pk_i \in Z[X]/(X^N - 1)$ for $j = 0,1, \dots, T-1$ constructs coefficient of polynomial values at $b(x)$ in $T-1$ is formulated by,

$$pk(x) = b_{0,} + \sum_{i=1}^{t-1} b_i x^i \tag{13}$$

For more dependencies to access rights to the users U_i, the key gets randomized to be generated by owner policy $H\left\{id_{i,} H(r_i), v_i k_{Loc_i}, \left[t_{a_i} t_{b_i}\right]\right\}$ and generates the sub-key x_i for U_i using (11). O broadcasts the data through the owner by representing to user B by attaining $\{id_i, x_i, H\ (id_i || r_i), H(Loc_i, \left[t_{a_i} t_{b_i}\right], A)\ )\}$ for secured access.

$$x_i = b(r_i) = \sum_{i=0}^{T-1} b_i \cdot r_j{}^i \tag{14}$$

3.3.2. Message Certificate Construction

By choosing the security parameters, randomly point the key at each message $\varphi \in l_\varphi$ and $E_m = \{E_{m_1}, \dots E_{m_i}, \dots, E_m\}$, where $E_{m_i} \in Z[X]/(X^N - 1)$, Then it generates the certificate (E_{m_i}, D_{m_i}) for message $S_i \in S$ by () where $1 \le i \le M$,

$$D_{m_i} = p\varphi * f + E_{m_i}(|q|) \tag{15}$$

After message construction, the data owner publishes the data to all users B using. $E_{m_i} = E_{m_1}, E_{m_2}, \dots E_{m_i}, \dots, E_{m_M}$ to encrypt the data.

3.3.3. Data Encryption

During the transmission, the data gets secured by encryption to process the cipher text $K = \{k_1, k_2, \dots, k_i, \dots, k_M\}$ for constructing messages $S = \{S_1, S_2, \dots, S_i, \dots, S_m\}$ as same k_i is the ciphertext of S_j To keep in a centralized server.

$$k_i = S_i \oplus H\left(b_0 * d_j\right) \tag{16}$$

Lets $H_1(S_i)$ attained by the owner to hold the keys $k_i, i = 1,2, \dots M$, in the storages. The system-building processes in Sub-Key Construction Message Certificate Construction and Data Encryption are shown in Algorithm 2.

Algorithm 2 Proposed system construction

Step 1: The polynomial factb (x) according to (13) in sub key constructed by the owner
Step 2: For each user U_i in B
Step 3: The chosen number r_i is encrypted with to generate key pk to get v_i and v_j by owner
Step 4: The owner Calculates $H' = H(r_i)$ and sends $\{id_i, H', v_i, v_j\}$.
Step 5: To process decrypts v_i, v_j to get the number r_i, using Algorithm 1
Step 6: If $H' = H(r_i)$
Step 7: If $r_i \neq r_\sigma$ for whichever U_σ the sub-key x_σ is received
Step 8: Based on the subkey sub-key x_i using (14) get retained;
Step 9: Compute broadcasting message be through $\{id_i, x_i, H\ (id_i || r_i), H(Loc_i, \left[t_{a_i} t_{b_i}\right], A)\ )\}$ to all users in B;
Step 10: Else
Step 11: They attain the request U_i to select dissimilar attribute number r_i and repeat Step 3;
Step 12: End If
Step 13: Else
Step 14: The message m is falsified;
Step 15: Re-converts $\{id_i, H', v_i, v_j\}$;
Step 16: Return Step 5;
Step 17: End If
Step 18: End For
Step 19: The data owner chooses parameters $\phi \in L_\phi E_m = \{E_{m_1}, \dots E_{m_i}, \dots, E_m\}$
Step 20: For each message $S_j \in S$
Step 21: The certificate signing be generated (E_{m_i}, D_{m_i}) for S_j by (15);
Step 22: To encrypt the data S_j by (16) to get k_i and calculates $H_1(S_j)$;
Step 23: They distribute E_{m_i} and keep k_i in storage.
Step 24: End For

3.3.4. Message Reconstruction

To reconstruct the data, the create mutual verification between the user U_i and $t-1$ other users to support U_i Regulating the data based on the access policy depends on location and time.

3.3.5. Certificate Processing

Based on the user request, the exchange certification is requested using access policies. The user gets a response based on the request U_j to send to the owner to access S_i's message certificate D_{m_i} were the data encrypted by the owner D_{m_i} using U_j' s secret number r_i.

The encryption was carried out by advanced encryption standard (AES) followed by the equation,

$$C_{D_{m_i}} = AES_{r_i}(D_{m_i}) \tag{17}$$

Requesting the cipher text $C_{D_{m_i}}$ to the owner, they are receiving $U_j$to decrypt the data. $C_{D_{m_i}}$ to attainD_{m_i} . By attaining practices, its sub-key x_i to calculate the conversationW_{ij} via (18) and sends $W_{ij}$to supplementary users in B.

$$W_{ij} = x_i * D_{m_i} \tag{18}$$

Certificate Verification

Using the public key e_j to verifyW_{ij} *basd on* (18) and (19) the validation $U_j$is confirmed byU_σ, form validated message m in $S_i$in U_σ *then* U_σ to assigns $\{id_\sigma, r_\sigma\}$ to U_j for certificate verification.

$$W_{ij} = xi * e_j \tag{19}$$

Reconstruction Message

By identifying the authenticated users have access rights $T-1$ to the user U_j as a legal rights B. They are retaining to reconstruct based on a non-sophisticated message. S_iBased on the following equation (20).

$$S_i = k_i \oplus H(\left(\sum_{U_j \in B} x_i \prod_{U_\sigma \in B, U_\sigma \neq U_j} \frac{r_\sigma}{r_\sigma - r_j}\right) * \tag{20}$$

Security Policy Update

In this stage, optimal security was achieved to secure the message in the storage. Depending on user access rights, the strategy is updated to the cloud server to give access rights,

$$k_{iv}^{j} = H(pk_0 * D_{m_i}) \oplus H({pk'}_0 * {D_{m_i}}') \tag{21}$$

The encrypted data k_i will be updated by getting the owner D rights which sends k_{iv}^{j} to the cloud server.

$${k_i}' = k_i \oplus k_{iv}^{j} \tag{22}$$

The cloud server then transmits k I' to the data owner is responsible for confirming that the generated cipher text from the new access policy has been correctly updated. The data owner can carry out this method. (23)

$$H_1(S_i) = H_1({k_i}' \oplus H({pk'}_0 * {D_{m_i}}') \tag{23}$$

The below algorithm 3 summarises Message reconstruction and exchange certificate computation and certificate verification.

Algorithm 3 Reconstruction and Verification

Step 1: Compute the cloud server; the user U_j get a request with key k_j through request D_{m_i} to data owner to secure data
Step 2: Encrypted data as cipher text$C_{D_{m_i}}$*by owner*, and to send the cypher text to the user $C_{D_{m_i}}$to U_j.
Step 3: Using the secret key r_i the user U_j decrypts data D_{m_i}*through* $C_{D_{m_i}}$
Step 4: $U_j$computes the exchange certificate W_{ij}via (18), and sends W_{ij} to other users in B;
Step 5: For each user U_σ in B Do
Step 6: Upon receiving W_{ij}, U_σ verifies $W_{ij}$by (19);
Step 7: If (20) holds
Step 8: U_σ sends its $(id_\sigma, r_\sigma, Loc_\sigma, [t_{a_\sigma} t_{b_\sigma}]$ to U_σ;
Step 9: Upon they receiving $(id_\sigma, r_\sigma, Loc_\sigma, [t_{a_\sigma} t_{b_\sigma}]$, U_j computes $H(id_\sigma || r_\sigma || Loc_\sigma || [t_{a_\sigma} t_{b_\sigma}])$ to verify $(id_\sigma, r_\sigma, Loc_\sigma, [t_{a_\sigma} t_{b_\sigma}])$.;
Step 10: If $H(id_\sigma || r_\sigma || Loc_\sigma || [t_{a_\sigma} t_{b_\sigma}])$ passes the verification
Step 11: U_σ participates in the reconstruction of S_i;
Step 12: EndIf
Step 13: End If
Step 14: End For
Step 15: The $t-1$ attained by recover S_i be accesed by other users 'B'.
Step 16: U_j regenerate process S_i via (21);
Step 17: End If

4. Simulation Results

The existing SVACS and ABAC structures are attaining API 3.0.3 in this research, and their competence is compared to the new SSVA-ACS system. Encrypted data, decryption time, policy update time, and policy verification time are all factors in the comparison. The number of translation nodes, defined as the total digit of users provided in the entrée tree structure, is contrasted with the different performance parameters in this scheme.

4.1. Encryption Time (s)

Table 1 depicts the encryption time for SVACS, ABAC and proposed SSVA-ACS schemes under the Number of Translation Nodes.

Table 1. Encryption time vs Number of translation nodes

Number of Translation Nodes	Encryption Time (s)		
	SVACS	ABAC	SSVA-ACS
2	150	140	133
4	145	138	129
6	152	145	137
8	155	148	136
10	147	139	130

The execution time on encryption using SVACS, ABAC and SSVA-ACS schemes for the Number of Translation Nodes is revealed in Number 4.1. When the number of translation nodes is 10, the encryption time of the proposed SSVA-ACS is 11.56% less than SVACS and 6.47% less than the ABAC structure. This analysis demonstrates that the projected SSVA-ACS scheme has better encryption time under the different number of translation nodes than SVACS and ABAC schemes.

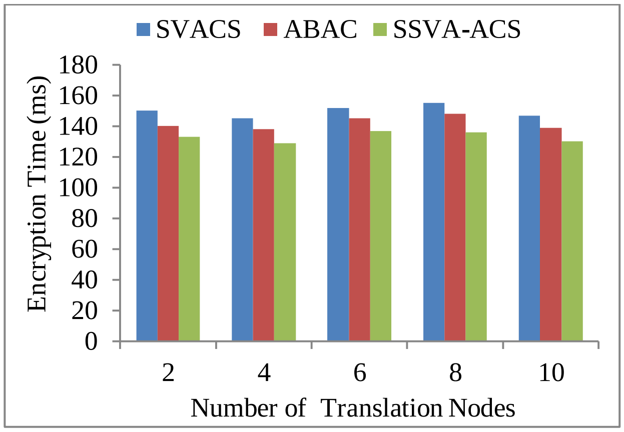

Fig. 1 Comparison of encryption time (s)

4.2. Decryption Time (s)

Table 2 depicts the decryption time for SVACS, ABAC and proposed SSVA-ACS schemes under the Number of Translation Nodes.

Table 2. Decryption time vs Number of translation nodes

Number of Translation Nodes	Decryption Time (s)		
	SVACS	ABAC	SSVA-ACS
2	149	135	123
4	151	149	130
6	150	141	134
8	152	142	132
10	148	137	127

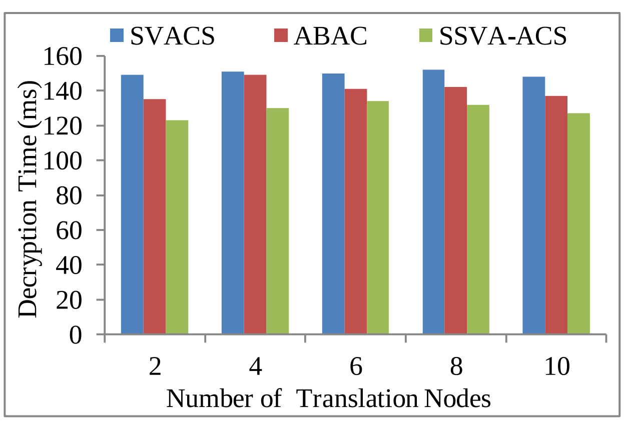

Fig. 2 Comparison of decryption time (s)

The execution time on decryption using SVACS, ABAC and SSVA-ACS schemes for the Number of Translation Nodes is shown in Figure 2.

When the number of translation nodes is 10, the Decryption time of the proposed SSVA-ACS is 14.18% less than SVACS and 7.29% less than the ABAC scheme. Figure 2 shows that the projected SSVA-ACS scheme has better Decryption time under the different number of translation nodes than SVACS and ABAC schemes.

4.3. Policy Update Time (s)

Table 3 depicts the decryption time for SVACS, ABAC and proposed SSVA-ACS schemes under the Number of Translation Nodes. The execution time on the policy update using SVACS, ABAC and SSVA-ACS schemes for the Number of Translation Nodes is exposed in Figure 3. When the number of translation nodes is 10, the policy update time of the proposed SSVA-ACS is 12.83% less than SVACS and 5.83% less than ABAC arrangement. This analysis shows that the projected SSVA-ACS scheme has better policy update time under the different number of translation nodes than the SVACS and ABAC scheme.

Table 3. Policy update time (s) vs Number of translation nodes

Number of Translation Nodes	Policy Update Time (s)		
	SVACS	ABAC	SSVA-ACS
2	156	146	131
4	150	141	133
6	149	140	129
8	153	145	132
10	148	137	129

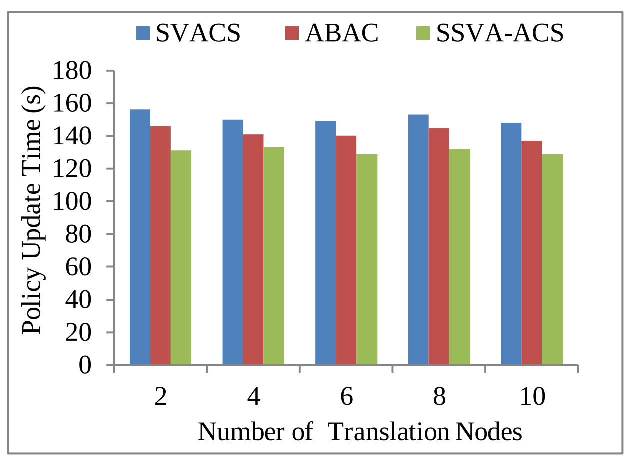

Fig. 3 Comparison of policy update time (s)

4.4. Policy Verification Time (s)

Table 4 depicts the policy verification time for SVACS, ABAC, and proposed SSVA-ACS schemes under the Number of Translation Nodes. The execution time on policy verification sings SVACS, ABAC and SSVA-ACS schemes for the Number of Translation Nodes is shown in Figure 4.

When the number of translation nodes is 10, the policy verification time of the proposed SSVA-ACS is 11.49% less than SVACS and 6.38% less than the ABAC scheme. This analysis shows that the projected SSVA-ACS scheme has better policy verification time under the different number of translation nodes than SVACS and ABAC schemes.

Table 4. Policy verification time (s) vs Number of translation nodes

Number of Translation Nodes	Policy Verification Time (s)		
	SVACS	ABAC	SSVA-ACS
2	146	136	126
4	150	142	133
6	152	149	139
8	147	138	130
10	149	141	132

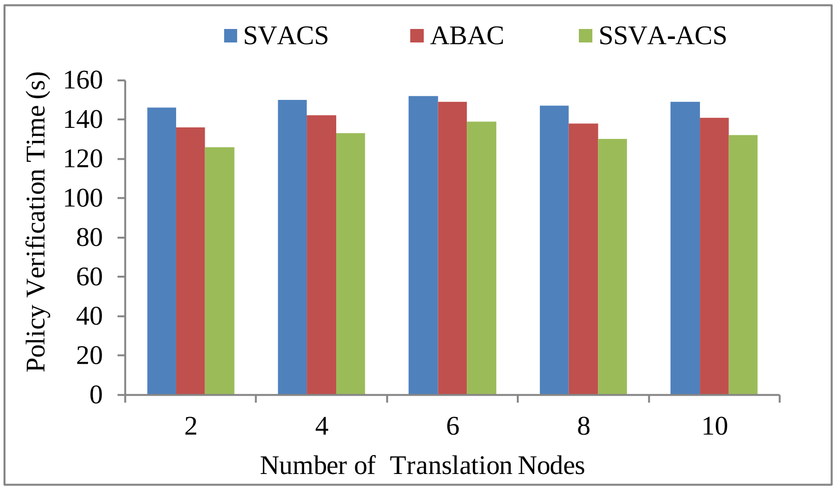

Fig. 4 Comparison of policy verification Time (s)

5. Conclusion

An INTRU cryptosystem based on spatial-temporal constrained ABAC is proposed in this paper to handle and secure massive data stored on cloud servers. First, update and validate the access policies to improve authorization flexibility and, as a result, resource usage and business timeliness. Then, not only does Our Mechanism provide attribute-based access control, but both INTRU and ABAC allow users to obtain encrypted text from CSs that are associated with a place and a valid time interval. It is also difficult to audit for compliance concerns because the user must check each object against your access policy rather than simply checking what access a specific user.

We also propose that an SSVAABAC be started using the Concrete Construction Encryption Mechanism to link a user's time-related privilege to the current access time. Finally, we provide a simulation analysis that supports its viability. As a result, we believe our work will help with cloud server building and reconstruction.

References

[1] Zhifeng Xiao, and Yang Xiao, "Security and Privacy in Cloud Computing," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 2, pp. 843-859, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[2] Rajkumar Kannan et al., *Managing and Processing Big Data in Cloud Computing*, IGI Global, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[3] Huaglory Tianfield, "Security Issues in Cloud Computing," *2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Seoul, Korea (South), pp. 1082-1089, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[4] Yunchuan Sun et al., "Data Security and Privacy in Cloud Computing," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, pp. 1-9, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sridhar Vemula, Ram Mohan Rao Kovvur, and Dyna Marneni, "CryptNoSQL – A Methodology for Secure Querying and Processing of Encrypted NoSQL Data on the Cloud Environment," *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 5, pp. 14-27, 2023. [CrossRef] [Publisher Link]

[6] Syed Asad Hussain et al., "Multilevel Classification of Security Concerns in Cloud Computing," *Applied Computing and Informatics*, vol. 13, no. 1, pp. 57-65, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] K. Radha et al., "Service Level Agreements in Cloud Computing and Big Data," *International Journal of Electrical and Computer Engineering*, vol. 5, no. 1, pp. 158-165, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ashutosh Kumar, "Quality and Security in Big Data: Challenges as opportunity to Make a Powerful Conclude Clarification," *International Journal of P2P Network Trends and Technology*, vol. 10, no. 3, pp. 10-17, 2020. [Google Scholar] [Publisher Link]
[9] Abhishek Gupta et al., "Information Assurance via Big Data Security Analytics," *International Journal of Computer & Organization Trends (IJCOT)*, vol. 5, no. 2, pp. 85-91, 2015. [Publisher Link]
[10] Rishav Chatterjee, and Sharmistha Roy, "Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud," *International Journal of Engineering Science and Computing*, vol. 7, no. 5, pp. 11818-11821, 2017. [Google Scholar] [Publisher Link]
[11] D. Shravani, "Review of Literature on Web Services Security Architecture Extended to Cloud, Big Data and IOT," *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 6, no. 4, pp. 7-12, 2016. [Publisher Link]
[12] D. Shravani, "Model Driven Architecture Based Agile Modelled Layered Security Architecture for Web Services Extended to Cloud, Big Data and IOT," *International Journal of Computer & Organization Trends (IJCOT)*, vol. 6, no. 4, pp. 55-64, 2016. [Google Scholar] [Publisher Link]
[13] Chunqiang Hu et al., "A Secure and Verifiable Access Control Scheme for Big Data Storage in Clouds," *IEEE Transactions on Big Data*, vol. 4, no. 3, pp. 341-355, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[14] Adeline Langlois, Damien Stehlé, and Ron Steinfeld, "GGHLite: More Efficient Multilinear Maps from Ideal Lattices," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 239-256, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[15] Sanjam Garg, Craig Gentry, and Shai Halevi, "Candidate Multilinear Maps from Ideal Lattices," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 1-17, 2013. [CrossRef] [Google Scholar] [Publisher Link]
[16] Kritika Soni, and Suresh Kumar, "Comparison of RBAC and ABAC Security Models for Private Cloud," *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing(COMITCon)*, Faridabad, India, pp. 584-587, 2019. [CrossRef] [Google Scholar] [Publisher Link]
[17] Zechao Liu et al., "A Temporal and Spatial Constrained Attribute-Based Access Control Scheme for Cloud Storage," *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, New York, USA, pp. 614-623, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[18] Zhiquan Lv et al., "Efficiently Attribute-Based Access Control for Mobile Cloud Storage System," *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Beijing, China, pp. 292-299, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[19] Joonsang Baek et al., "A Secure Cloud Computing-Based Framework for Extensive Data Information Management of the Smart Grid," *IEEE Transactions on Cloud Computing*, vol. 3, no. 2, pp. 233-244, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[20] Kan Yang et al., "Enabling Efficient Access Control with Dynamic Policy Updating for Big Data in the Cloud," *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, Toronto, Canada, pp. 2013-2021, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[21] Gaoqiang Zhuo et al., "Privacy-Preserving Verifiable Data Aggregation and Analysis for Cloud-Assisted Mobile Crowdsourcing," *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, San Francisco, CA, USA, pp. 1-9, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[22] M. H. Xing, and W. M. Li, "An Attribute-Based Access Control Scheme in the Cloud Storage Environment," *Software Engineering and Information Technology*, pp. 129-134, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[23] Rohit Ahuja, and Sraban Kumar Mohanty, "A Scalable Attribute-Based Access Control Scheme with Flexible Delegation Cum Sharing of Access Privileges for Cloud Storage," *IEEE Transactions on Cloud Computing*, vol. 8, no. 1, pp. 32-44, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[24] K. Rajalakshmi et al., "An Effective Approach for Improving Data Access Time using Intelligent Node Selection Model (INSM) in Cloud Computing Environment," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 5, pp. 174-184, 2023. [CrossRef] [Google Scholar] [Publisher Link]
[25] Banoth SeethaRamulu, H. Balaji, and Bashetty Suman, "Attribute Based Access Control Scheme in Cloud Storage System," *International Journal of Engineering & Technology*, vol. 7, no. 4.6, pp. 33-35, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[26] Heng He et al., "An Efficient Attribute-Based Hierarchical Data Access Control Scheme in Cloud Computing," *Human-Centric Computing and Information Sciences*, vol. 10, no. 1, pp. 1-19, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[27] Hanshu Hong, and Zhixin Sun, "A Flexible Attribute Based Data Access Management Scheme for Sensor-Cloud System," *Journal of Systems Architecture*, vol. 119, p. 102234, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[28] Mariem Bouchaala, Cherif Ghazel, and Leila Azzouz Saidane, "TRAK-CPABE: A Novel Traceable, Revocable and Accountable Ciphertext-Policy Attribute-Based Encryption Scheme in Cloud Computing," *Journal of Information Security and Applications*, vol. 61, p. 102914, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[29] S. Veerapandi, R. Surendiran, and K. Alagarsamy, "Live Virtual Machine Pre-copy Migration Algorithm for Fault Isolation in Cloud Based Computing Systems," *DS Journal of Digital Science and Technology*, vol. 1, no. 1, pp. 23-31, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] S. Veerapandi, R. Surendiran, and K. Alagarsamy, "Enhanced Fault Tolerant Cloud Architecture to Cloud Based Computing using Both Proactive and Reactive Mechanisms," *DS Journal of Digital Science and Technology*, vol. 1, no. 1, pp. 32-40, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Qian Xu et al., "Decentralized and Expressive Data Publish-Subscribe Scheme in Cloud Based on Attribute-Based Keyword Search," *Journal of Systems Architecture*, vol. 119, p. 102274, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[32] Prabhu Shankar et al., "Energy-Efficient Data Offloading using Data Access Strategy-Based Data Grouping Scheme," *SSRG International Journal of Electronics and Communication Engineering*, vol. 10, no. 5, pp. 28-37, 2023. [CrossRef] [Publisher Link]