International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Securing Cloud Data: An Enhanced Approach through Attribute-Based Access Control Mechanism

K. Raja[1], Dr. K. Sujith[2]
[1]Research Scholar, Department of Computer Science, Annai College of Arts & Science (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, Tamilnadu, India.
[2]Associate Professor, Department of Computer Science, Annai College of Arts & Science (Affiliated to Bharathidasan University, Tiruchirappalli), Kovilacheri, Kumbakonam, Tamilnadu, India.

Abstract: Cloud computing is considered one of the most dominant paradigms in the Information Technology (IT) industry these days. It offers new cost-effective services on-demand such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). However, with all of these services promising facilities and benefits, there are still a number of challenges associated with utilizing cloud computing such as data security, abuse of cloud services, malicious insider and cyber-attacks. Among all security requirements of cloud computing, access control is one of the fundamental requirements in order to avoid unauthorized access to systems and protect organizations assets. Although, various access control models and policies have been developed such as Attribute based Access Control (ABAC) and Role Based Access Control (RBAC) for different environments, these models may not fulfil cloud's access control requirements. In this paper, an enhanced attribute-based access control based on strategy mechanism is proposed by introducing a strategy for providing access control to the users in the cloud environment.

Keywords: Cloud computing, Access Control, Security, Attribute based Access Control, Encryption, Decryption, time consumption.

1. INTRODUCTION

Cloud computing is an open standard model, which can enable ubiquitous computing and offer on-demand network access to a shared pool of configurable computing resources. It is Internet-centric and provides all of its resources as services such as storage, computation and communication. Cloud computing is a unique combination of capabilities and innovation technologies. It needs minimal management effort from service providers [1] and delivers scalable and dynamic infrastructure, global/remote access and usage control and pricing. Almost three-fourths of 572 surveyed business leaders, indicate that their companies have piloted, adopted or considerably implemented cloud computing in their organizations and 90% expect to have done so in next three years. Moreover, those companies who have substantially implemented cloud computing are expected to grow from 13% to 41% within the next three years [2].

Security is one of the primary concerns and a major barrier to adopt cloud computing. Cloud computing may suffer from conventional distributed systems' security attacks such as malicious code (Viruses, Trojan Horses), back door, Man-in the Middle attack, Distributed Denial-Of-Service (DOS) attack, insecure application programming interface, abuse and nefarious use of cloud computing and malicious insiders. Cloud services could be inaccessible due to these attacks and generate negative impact. It is an important and primary requirement for cloud service providers to ensure its services are fully usable and available at all time [3]. Moreover, cloud computing has brought new concerns such as moving resources and storing data in the cloud with probability to reside in another country, which has different regulations. Furthermore, cloud computing is a shared environment, which uses sharing infrastructure. Hence, data may face issues like privacy and unauthorized access. These issues can get more complicated when different service providers use various types of technologies and cause potential heterogeneity issues [4]. Furthermore, virtualization brings its own issues such as data leakage.

2. IMPORTANCE OF ACCESS CONTROL

In the cloud environment, the sensitive, large, scalable, stored data requires a secure manner to protect and preserve its integrity and confidentiality without affecting the scalability and the performance of the system. One of the critical security mechanisms for data protection is access control that permits, restricts or denies access to system files by setting some conditions and rules which are combined together to make and enforce an access control decision [5]. In this way, the access control technique can ensure only authorized users who need to access certain data, have the ability to do that.

Some core requirements need to be achieved in any effective cloud access control system. The first one is fine-grained access control [6]. In particular, each user in a system has their own access right which may differ from others in the same group. Due to lack of control, the second requirement is to assign control to the data owners after residing their data on the cloud without computation overhead which is the third requirement. To keep data safe and guarantee the security, the data has to be encrypted. That will keep data away from being illegitimately accessed by a cloud server or any unauthorized users. Therefore, the fourth requirement is confidentiality [7].

To meet the above requirements, attribute-based access control has been introduced [8]. However, to hide the data from a storage server, encrypting data is essential before storing them on such servers. Thus, data encryption with attribute-based access control is known as an Attribute-Based Encryption (ABE) technique. An attribute is a piece of information that describes the properties, features or characteristics of an object [9]. This information can be recognised by either automated or human approaches. For example, an attribute could be a department (e.g. engineering, computer science, etc.), an occupation (e.g. teacher, student, researcher, etc.), and experience years (e.g. two-years, five-years, etc.). In general, attributes are classified into two types [10]: 1) non-temporal attributes with discrete attribute values (e.g. age, address, email, etc.), and 2) temporal attributes with continuous values (e.g. interval, time, etc.).

Many studies have been carried out on the cloud access control using ABE with discrete attribute values [11][12]. These studies have a lot of problems which remain unsolved. For example, On the other hand, some schemes require intensive computations in return for stronger privacy and security protection, meaning that they are unsuitable for mobile devices with limited computation power [13][14].

In addition, some work has been carried out using ABE with continuous attribute values, which is known as temporal access control [15][16]. The access structure can be in the form of time (e.g. between 8 am and 12 pm). These temporal attributes are familiar in the cloud. For instance, only during a particular period of time, can users access certain data. However, such schemes have their shortcomings.

Achieving data confidentiality and access control for the cloud data is a core challenge that needs to be taken into account. Addressing this challenge supports data security management, and allows data owners to regulate their data and enforce restrictions on accessing data. Traditional cryptographic techniques can keep data confidentiality.

3. PROPOSED STRATEGY BASED ACCESS CONTROL MECHANISM FOR ENHANCING THE CLOUD SECURITY

The proposed Strategy based Access Control approach composed of the following Algorithms:

Step 1: Initialization of the Parameters

Step 1.1: Input: Number of Authorities and security parameters.

Step 1.2: Output: The generation of Master key and Public Key – Equation (1) & (2).

Step 1.3: The authority chooses the master key as the secret key.

Step 1.4: The authority chooses the prime order and the bilinear group.

Step 1.5: The number of attributes in the authority are generated by the bilinear group.

Step 1.6: The cryptographic hash function is defined.

$$PK = e(g,g)^{a}, g^{\alpha}, H, g, g^{\beta}, g^{\gamma}, h, h_1, \ldots., h_U \qquad (1)$$

$$MK = \alpha, \beta, \gamma \qquad (2)$$

Step 2: Encryption

Step 2.1: Input: Public Key, Access Structure, and Message.

Step 2.2: Output: Cipher Text of the Message.

Step 2.3: The rows of the message is considered as the attributes.

Step 2.4: The message is considered as the l3n Matrix.

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Step 2.5: Then the random vector is chosen which is utilized to share the exponent for encryption.

$$CT = \left\{ \begin{matrix} C = Me(g,g)^{\alpha s}, C' = \ g^{s}, C'' = \ g^{\beta s}, C''' = \\ g^{\gamma s}, \left(C_1 = \ g^{a\lambda_1} h_{p(1)}^{-r_1}, D_1 = g^{r_1}\right), \ldots, \\ \left(C_1 = \ g^{a\lambda_1} h_{p(l)}^{-r_1}, D_1 = g^{r_1}\right) \end{matrix} \right\} \qquad (3)$$

Step 3: Key Generation

Step 3.1: Input: Global Identifier, Master key, and the attributes set.

Step 3.2: Output: Generation of Private Key

Step 3.3: The equation (4) used to generate the private key with GID, attributes sets and the master key.

$$K = g^{\alpha} g^{at} h^{u\beta}, L_2 = h^{\gamma}, K_x = h_x^t, \forall x \in S_1 \quad (4)$$

Step 4: Output Key Generation

Step 4.1: Input: In this step, the private key generated in the previous step 3 is considered as the input.

Step 4.2: Output: The generations of the outsourced key and the retrieve key.

Step 4.3: In this step, the random values is chosen by the user.

Step 4.4: Using the random values, the retrieve key is generated using equation (5) and (6). Then the outsourced key is also published.

$$K' = g^{\alpha/z} g^{at/z} h^{u\beta/z}, L_1' = g^{t/z}, L_2' = h^{\gamma/z} \quad (5)$$

$$L_3' = h^{u/z}, K_x' = h_x^{t/z}, \forall x \in S_1 \qquad (6)$$

Step 5: Transform Key Generation

Step 5.1: Input: Step (3) key generation and Step (2) encryption.

Step 5.2: Output: The Generation of Transform key.

Step 5.3: The key generation algorithm is called by the authority to generate the key for new attribute set.

Step 5.4: Then the encryption algorithm is used to encrypt the message with attribute sets and with access structure, to generate the transform key.

$$T = g^{\alpha} g^{at'} h^{H(d_1),H(d_2)}, T' = g^{t'}, T_x = h_x^{t'}, \forall x \in S_1 \qquad (7)$$

$$T'' = En_{A_2}(d_1, d_2) \qquad (8)$$

Step 6: Re-Encryption

Step 6.1: Input: Cipher Text association with first access structure and Transformation Key.

Step 6.2: Output: Generation of the Updated Cipher Text

Step 6.3: The updation of the cipher text is done with the access structure which is satisfied by the attribute set, and with the set of constants.

Step 6.4: The below equations (9),(10) and (11) are used to update the cipher text.

$$C_1' = Me(g,g)^{\alpha s}, C_3' = \ En_{A_2}(d_1, d_2), C_4' = g^{s} \qquad (9)$$

$$C_2' = \frac{e(C',T)}{\prod_{i \in I}\left(e(C_i,T')e\left(D_i,T_{\rho(i)}\right)\right)^{\omega_i}} \qquad (10)$$

$$= e(g,g)^{\alpha s} e(g,h)^{sH(d_1)H(d_2)} \qquad (11)$$

Step 7: Decryption

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Step 7.1: Input: The private key and the updated cipher text.

Step 7.2: Output: Plain text or symbol message.

Step 7.3: The decryption of the cipher text takes place if the access structure with the cipher text is satisfied by the attribute key.

Step 7.4: The equation $e(L_2, C^{tu}) = e(h^u, C''')$ is used to check the correct authority. If the verification is not passed, then the key is generated from the malicious authority, then the process is stopped.

Step 7.5: The computation of the key is done with equation (12) in the figure 7.

Step 7.6: The equation (13) is used to decrypt the original message.

$$\frac{e(C',K)}{e(h^u,C'')\prod_{i\in I}\left(e(C_i,L_1)e\left(D_i,K_{\rho(i)}\right)\right)^{\omega_i}} \qquad (12)$$

$$\frac{C_1'}{\left(C_2'/e\,(\pi)\left(C_4',h^{H(d_1)H(d_2)}\right)\right)} = M \qquad (13)$$

Step 8: Output Decryption

Step 8.1: Input: Cipher text, Outsourced key and the retrieve key.

Step 8.2: Output: Message or symbol.

Step 8.3: The Linear Secret Sharing Scheme (LSSS) is set as the threshold.

Step 8.4: The outsourced key is send for a set and the cipher text for the given access structure.

Step 9: Strategy to Update

Step 9.1: When the data owner wants to change the access policy from previous policy A to a new policy A, he first runs the update-key generation algorithm and then sends the updated keys to the cloud server.

Step 9.2: After receiving update keys, the cloud server executes the ciphertext-update algorithm to update the ciphertext.

4. RESULT AND DISCUSSION

In this research paper, a strategy Attribute based Access Control mechanism for the cloud storage system, which is both efficient and secure. In this section, the result obtained by the proposed policy-attribute based access control encryption, key generation and decryption time for the varying number of authorities and varying number of attributes in per authority. Table 1 depicts the computation time for the encryption, key generation and decryption for the varying number of authorities. Table 2 depicts the computation in seconds by the existing Attribute based Access Control for the encryption, key generation and decryption for the varying number of authorities. From the table 1, and table 2, it is clear that the computation time in second by the proposed SA-BAC takes minimal encryption time, key generation time and decryption time when it is compared with existing ABAC system.

Table 1: Computation time in seconds by the proposed SA-BAC system with varying number of authorities

Number of Authorities	Proposed Strategy- Attribute based Access Control- Computation time in Seconds		
	Encryption Time	Key Generation time	Decryption Time
2	12	18	16
3	18	28	21
4	22	37	32
5	25	49	39
6	29	54	49
7	38	65	56
8	52	72	68

9	64	78	75
10	78	85	82
11	85	92	93

Table 2: Computation time in seconds by the Existing Attribute based Access Control system with varying number of authorities

Number of Authorities	**Existing Attribute based Access Control - Computation time in Seconds**		
	Encryption Time	**Key Generation time**	**Decryption Time**
2	22	25	28
3	30	39	35
4	41	51	48
5	52	78	56
6	63	89	68
7	81	99	75
8	97	108	89
9	105	122	95
10	128	131	109
11	146	139	115

Table 3 depicts the computation time in seconds by the proposed SA-BAC system with varying number of attributes per authority. Table 4 depicts the computation time in seconds by the existing Attribute based Access Control system with varying number of attributes per authority. From the table 3, and table 4, it is clear that the computation time with varyining number of attributes per authority in second by the proposed SA-BAC takes minimal encryption time, key generation time and decryption time when it is compared with existing ABAC system.

Table 3: Computation time in seconds by the proposed SA-BAC system with varying number of attributes per authority

Number of Attributes per Authority	**Proposed Strategy - Attribute based Access Control- Computation time in Seconds**		
	Encryption Time	**Key Generation time**	**Decryption Time**
6	21	21	18
8	29	32	28
10	35	46	39
12	51	59	48
14	63	70	64
16	75	89	75
18	89	97	88
20	97	101	97
22	101	119	105
24	112	121	116

Table 4: Computation time in seconds by the existing Attribute based Access Control system with varying number of attributes per authority

Number of Attributes per Authority	**existing Attribute based Access Control - Computation time in Seconds**		
	Encryption Time	**Key Generation time**	**Decryption Time**
6	35	38	26
8	48	54	39

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

10	68	71	56
12	79	92	72
14	92	105	89
16	118	118	98
18	129	126	110
20	135	138	128
22	147	145	139
24	163	167	156

5. CONCLUSION

Cloud Computing is an emerging technology now a days, where cloud is most preferable when there is data backup, storage and data distribution service with low cost. But cloud is semi honest in nature due to not reveled storage and security structure thus while storing and sharing cloud data, its suppose to honest and secured. When data owners outsource their data in secured manner system should assure the security, data integrity and confidentiality. Here we noticed secure access controlling is the prime objective for sensitive data management. Through this research work, attribute-based access control based on Strategy is proposed. The proposed SA-BAC system consumed less encryption time, key generation time and decryption time when it is compared with existing attribute-based access control system.

REFERENCE

[1] Geelan, Jeremy. "Twenty-one experts define cloud computing. Virtualization." Electronic Magazine, http://virtualization. sys-con. com/node/612375 (2008).

[2] Li, Xinlu, and Xiaoxia Zhao. "Survey on access control model in cloud computing environment." 2013 International Conference on Cloud Computing and Big Data. IEEE, 2013.

[3] Li, Xiao-Yong, et al. "Multi-tenancy-based access control in cloud." 2010 International Conference on Computational Intelligence and Software Engineering. IEEE, 2010.

[4] Almutairi, Abdulrahman, et al. "A distributed access control architecture for cloud computing." IEEE software 29.2 (2011): 36-44.

[5] A. R. Khan, "Access control in cloud computing environment," ARPN Journal of Engineering and Applied Sciences, vol. 7, no. 5, pp. 613-615, 2012.

[6] C.-W. Liu, W.-F. Hsien, C. C. Yang, and M.-S. Hwang, "A survey of attribute- based access control with user revocation in cloud data storage," IJ Network Security, vol. 18, no. 5, pp. 900-916, 2016.

[7] M. Ahmadi, M. Chizari, M. Eslami, M. J. Golkar, and M. Vali, "Access control and user authentication concerns in cloud computing environments," in Telematics and Future Generation Networks (TAFGEN), 2015 1st International Conference on, 2015: IEEE, pp. 39-43.

[8] S. Ruj, "Attribute based access control in clouds: A survey," in Signal Processing and Communications (SPCOM), 2014 International Conference on, 2014: IEEE, pp. 1-6.

[9] V. C. Hu et al., "Guide to attribute-based access control (ABAC) definition and considerations (draft)," NIST special publication, vol. 800, no. 162, 2013.

[10] M. Thangavel and P. Varalakshmi, "A survey on security over data outsourcing," in 2014 Sixth International Conference on Advanced Computing (ICoAC), 2014: IEEE, pp. 341-349.

[11] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 384-394, 2014.

[12] K. Yang and X. Jia, "DAC-MACS: Effective data access control for multi- authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 59-83, 2013.

[13] S. M. Khan and K. W. Hamlen, "AnonymousCloud: A data ownership privacy provider framework in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012: IEEE, pp. 170-176.

[14] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "A practical privacy- preserving password authentication scheme for cloud computing," in Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, 2012: IEEE, pp. 1210-1217.

[15] K. Yang, Z. Liu, Z. Cao, X. Jia, D. S. Wong, and K. Ren, "TAAC: Temporal attribute-based access control for multi-authority cloud storage systems," IACR Cryptology EPrint Archive, vol. 2012, p. 651, 2012.

[16] Y. Zhu, H. Hu, G.-J. Ahn, D. Huang, and S. Wang, "Towards temporal access control in cloud computing," in INFOCOM, 2012 Proceedings IEEE, 2012: IEEE, pp. 2576-2580.