Research Article

Secure Information in Cloud Storage Using Hierarchical-authority Attribute-Based Encryption (HABE): A Literature Review

Arief Arfriandi*, Rahmat Gernowo, and R Rizal Isnanto

Doctoral Program of Information System, School of Postgraduate Studies, Universitas Diponegoro, 50275, Central Java, Indonesia

ORCID
Arief Arfriandi: https://orcid.org/0000-0002-5244-8208

Corresponding Author: Arief Arfriandi; email: ariefarfriandi@students.undip.ac.id

Published 12 March 2024

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICESRE Conference Committee.

Abstract.
Access control using hierarchical-authority attribute-based encryption (HABE) in securing information in cloud storage is one of the security methods that work to maintain information privacy through the management of access rights to encrypted information, thus preventing unauthorized users and systems from accessing stored information without permission. In this paper, we further explore one scheme that is a part of attribute-based encryption (ABE) for the process of securing data or information stored in cloud storage, namely HABE, which is a development of the ciphertext policy attribute-based encryption. Furthermore, this paper summarizes the advantages and weaknesses of HABE in securing information storage in the cloud and the direction of future research or HABE research trends. The method proposed in this paper is to explore the progress of research that has been done, and to classify access structures consisting of monotomic and non-monotomical, multi-authority schemes. Then it will also define functionality as well as performance on the cost of computing to know the advantages and disadvantages of each HABE when applied to the process of storing data or information in cloud storage. In its development, HABE, compared to Cypher Policy Attribute-Based Encryption (CPABE), has different characteristics. HABE provides full delegation and support for services on a larger scale, whereas CPABE, with its access structure, can define messages with better performance. With these results, it is expected that research related to HABE will be more focused on the development of HABE, as it is more appropriate to support the management of information security on a large scale.

Keywords: information security, CPABE, HABE, cloud storage

1. Introduction

Cloud computing provides new environments and new ways to exploit the resources or technological resources needed in business development. In a cloud environment, we use resources based on what is used, or pay by use [3]. These cloud environments include essential services including Platform as a Service (PaaS), which offers results from programming languages, Infrastructure as a Service (IaaS), and Software as a

How to cite this article: Arief Arfriandi*, Rahmat Gernowo, and R Rizal Isnanto, (2024), “Secure Information in Cloud Storage Using Hierarchical-authority Attribute-Based Encryption (HABE): A Literature Review” in 6th *International Conference on Education and Social Science Research*, KnE Social Sciences, pages 335–345. DOI 10.18502/kss.v9i6.15283

Service (SaaS), which provides an interface to cloud users. Applications of cloud models in running computing include private cloud, public cloud, community cloud, and hybrid cloud. Some of these cloud models are differentiated according to the owners and users of the cloud model.

Private cloud is owned by an organisation; public cloud is used by the public or multiple consumers; whereas a hybrid cloud combines public and private clouds. With a cloud, data or information on a large scale can also be stored in the cloud, but with security and privacy issues, there are still doubts among cloud users about storing data and information [4]. Cloud storage is storage in a cloud environment used to store data or information that can be managed remotely or accessible from anywhere [5]. When data or information is stored in cloud storage, the cloud storage provider can access and share the sensitive information stored with unauthorised parties. In order to maintain the security of data or stored information, and before being sent into the cloud, information must be encrypted with restricted access and user rights. So when storing data and information, there are two things to keep in mind: privacy and user access control [6].

The use of cryptography in securing data or information can be done with asymmetrical key encryption techniques. With an asymetric key, the encrypting and decryption processes use different keys so that privacy can be awakened but access controls cannot be overcome in cloud storage. To overcome this, use attribute-based encryptions, or attribute-based encryption (ABE), so that the decryptions can only be done by users who have the same attributes as the specified [7]. Key Policy Attribute-Based Encryption (KPABE) and Cypher Policy Attribute-Based Encryption (CPABE) are the two primary subtypes of ABE (8). At KPABE, the chipertext is generated based on an attribute, while the secret key is produced based on a specified policy. Another type of ABE is hierarchical-authority attribute-based encryption (HABE) [9] which is a development of the CPABE. In this paper, we explore and summarise the advantages and weaknesses of HABE in securing information stored in the cloud and give direction to the development of research or trends related to HABE.

2. Method

To determine the direction of further research related to the HABE used to secure data or information in cloud storage, the method presented in this paper is to explore the development of research that has been done related to CPABE and HABE and to classify access structures consisting of monotomic [1] and non-monotomic [2], and a multi-authority scheme. Then it will also define functionality as well as performance on the cost of computing to know the advantages and disadvantages of each HABE when applied to the process of storing data or information in cloud storage.

3. Result and Discussion

3.1. Result

Table 1 provides various general notations utilised in this paper related to the ABE method.

Table 1: Notation Used in The ABE Algorithm [8].

Notation	Meaning
P	prime order
G1, G2	prime order bilinear group
g, g1	creator of the group
d	criterion value
UA	universe of attributes
n	quantity of UA attributes
q, qx	random d-1 degree polynomial
AU	set of user attributes
c, r	random non-zero values from Zp
r0	root node of the access tree
x	the access tree’s node
т	access tree

3.1.1. CPABE

In CPABE, which is part of ABE, generating chipertext is done based on access policy, while the creation of a secret key is based on attributes. The CPABE scheme is shown in Figure 2.

On the ABE system, the process of decrypting data or encrypted information is carried out involving user attributes, and the user key is created based on a specified policy, while on the CPABE, the attribute is involved to decrypt user credentials, and the policy of who decrypts is made by the data encryption party [10]. The main components of CPABE include data owners, trusted parties, and data users [8], i.e.,

1. Trusted parties generate a master secret key (MSK) and a public key (PK). This PC serves to encrypt data or information. In the process of generating MSK and PK,

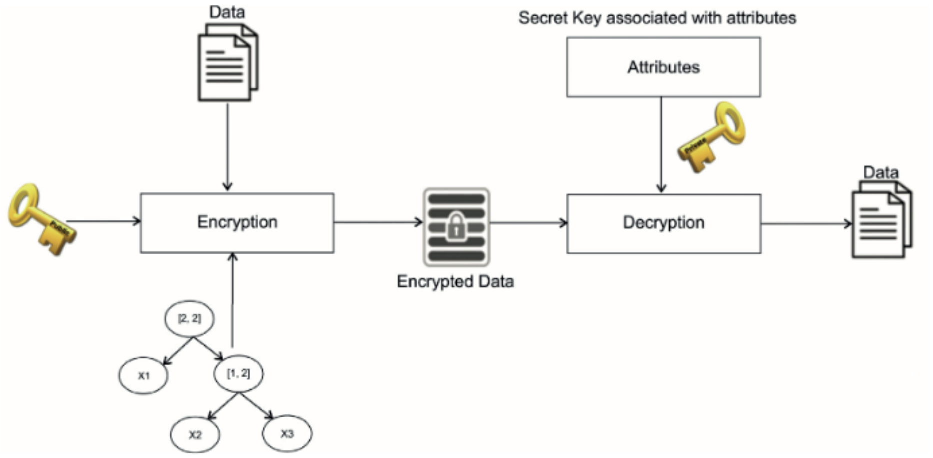


Figure 1: CPABE scheme [8].

random values are used instead of zero α, β from Z_p. PK and MSK shown on the equation (1),

$$PK = (G1,\ g,\ h = g\beta, f = g\frac{1}{\beta},\ l(g,\ g)^{\alpha}(1)$$

$$MSK = (\beta,\ g^{\alpha})$$

1. Design of a secret key (S) for a user involves MSK and a set of user attributes (AUs), thus generating a random value instead of zero r_a for each attribute a∈ AU. S shown on the equation (2),

$$S = \left(g^{\frac{\alpha+r}{\beta}}\right),\ \forall\alpha\ \in AU; D_{\alpha} =\ g^{r}.H(\alpha)^{r}_{\alpha},\ D^{\text{l}}_{\alpha} =\ g^{r}_{\alpha}(2)$$

2. The message encryption process (M) PK and access structure (т) are involved. for example $q_x(0) = q_{parents(x)}(\text{index}(x))$ and $q_{r0}(0)$ = S, where S ∈ Zp. If LN represents a collection of leaf nodes, then the definition of encrypted text E shown on the equation (3),

$$E \sim = Ml\ (g,\ g)^{\alpha s},\ E_1 =\ h^s,\ 6i\ \in LN,\ E_y =\ g^{q^{i(0)}},\ E^{i}_{y} =\ H(att(i))^{q^{(0)}}(3)$$

3. In the process of chipertext decryption, the user uses the user's secret key (S). If v = w = att(x) and count M if w ∈ AU, then the decryption process shown on the equation (4),

$$M =\ /\frac{l\left(D_{w,}\ \ E_v\right)}{l\left(D_{w^{\text{l}}},\ E_{v^{\text{l}}}\right)} =\ /\frac{l\left(g^{r}.\ H(W)^{r_{\alpha}},\ g^{q_v{}^{(0)}}\right)}{l\left(g^{r},\ H(W)^{q_v{}^{(0)}}\right)} =\ \ /\ l(g,\ g)^{rq_{v^{(0)}}}(4)$$

4. The delegation process uses a secret key (S) as an input and then, when necessary, re-creates a new key whenever a renewal is required. If A is an additional set of attributes, where A ⊆ AU. Then select a random value other than zero r$_{w}$ ’ ∈ Z$_{p}$for each attribute w ∈ AU, until the secret key (S) shown on the equation (5),

$$= (Sf,\ \forall w\ \in :_{w}=\ S_{w}.g.H(w)^{w},\ _{w} = S^{\text{l}}.g^{w}\ )\ (5)$$

This CPABE scheme has been improved and proved that the generated chipertext is safer. Improvements to such schemes for the first time involve Diffie-Hellman’s Bilinear Decisional (DBDH) [11]. Improvements to the CPABE scheme are being undertaken that support access trees with limited size [12]. With the access tree, the access management involved in the generate key and decryption process becomes more structured, but there are weaknesses in using this access tree associated with the limitation of the depth of the access tree, which can only be determined at the setup phase itself [13]. The CPABE efficiency level is further improved by adding boolean AND and OR operators with thresholds. In a single-authority CPABE scheme, this scheme will encounter obstacles when faced with different types of users that require different sets of attributes, so to overcome such a problem, use multi-authoritative CPABE [14].

Multi-authority: in the CPABE scheme, user attributes can be traced from their global identities and have low efficiency, thus being improved with new multi-authority by creating several central authorities that work ide-dependently and using monotomic access structures [15] as well as adding accountability to users [16]. With this multi-authority model, all such sets of attributes are then divided into several different sets, and the separated sets are assigned to each authority. The single authority issue still exists with this scheme, although it has been resolved by the CPABE scheme’s multi-authority threshold [17]. A secret key can only be derived from a single authority in a CPABE scheme model with a threshold since no one authority has complete control over any attribute once several such authorities are merged.

3.1.1.1 Hidden Policies

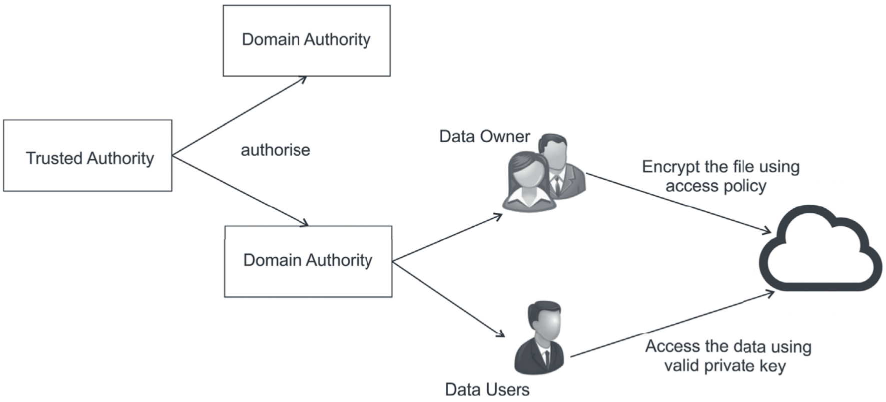
With the chipertext sent to the cloud storage, the access structure is then sent so that the access policy is accessible to anyone who accesses the chipertext. With all users able to know that access policy, it causes weak privacy policy. It’s fixed using hidden policies [18]. The predicate encryption technique and the AND gate on a multi-value attribute with a wildcard access structure are used in the CPABE scheme, thus obtaining hidden access preferences, but the increasing problem with the size of the chipertext remains. The problem is solved by sorting hidden policies based on public parameters and the length of the chipertext [19. 21]. The CPABE scheme with this hidden policy is then refined by shortening the chipertext using the positive AND, negative, and wildcard gates used on access structures [22].

3.1.1.2 Attribute based proxy re-encryption

When the data owner is offline or unable to complete the encryption procedure, the CPABE-based system works to delegate the data owner to re-encrypt data or information in accordance with the new access policy while still maintaining effective access control [23]. This scheme is enhanced by involving a re-encryption control that serves to determine whether or not the chipertext can be re-encrypted [24], however, there are still computational cost constraints due to the number of pairing operations required, so a model is proposed by minimising pairing operations with an exponential operation. [25]. attribute-based proxy re-encryption enhanced with LSSS access structure [26] and double encryption [27]. We employ weighted access tree architectures with OR, AND, and threshold gates to enhance efficiency and reduce processing costs [17].

3.1.2. HABE

The CPABE scheme can produce data or information encryption and can manage access control well. However, the CPABE scheme does not run optimally if used in large-scale companies because it only supports full delegation mechanisms. This weakness is improved by the HABE scheme, which uses universal attributes classified into a tree structure defined in the access policy [28]. The HABE scheme is shown in Figure ??.



1
2

Figure 2: HABE scheme (8).

3.2. Discussion

In Table 2, a comparison of the access structure, advantages, and disadvantages between CPABE and HABE based on recent research that has been conducted is shown, and a comparison of the functionality between CPABE and HABE is shown in Table 3. The security models of CPABE and HABE are shown in Table 4.

TABLE 2: Comparison Between CPABE and HABE [8].

Scheme	Access Structure	Advantages	Disadvantages
CPABE (17)	Monotomic	Reduced the computational cost of the private key and handle user revocation	Due to CA only providing users with all of the private keys, the central authority may decrypt all of the data
HABE (29)	Monotomic	Use of a single integrated access structure. Reduce the cost of storage and computational complexity	It does not support the method for revocation.

TABLE 3: Functionality Comparison Between CPABE and HABE [8].

Scheme	Fine-grained access control	Collusion resistant	Revocation mechanism	Scalability
CPABE	yes	yes	yes	no
HABE	yes	yes	yes (user)	yes

TABLE 4: Security Model Between CPABE and HABE [8].

Scheme	Security Model	Security assumption
CPABE (30)	Fully	Generic Group
HABE (31)	Fully	Generic Group

Table 5 displays the notations used for the performance analysis. Table 6 displays the computational cost performance, whereas Table 7 displays the storage cost and communication cost performance.

4. Conclusion

In its development, if compared between the HABE scheme and the CPABE, the two schemes have different characteristics. HABE provides full delegation and support for information security management services on a larger scale, while CPABE with its access structure can define messages with better performance. With these results, it is expected

Table 5: Notation On Performance Analysis [8].

Notations	Meaning
η_{UA}	amount of common attributes
η_{u}	amount of users
η_{∂}	numerous user attributes
η_{ι}	amount of ciphertext attributes
η_{nln}	the access tree's non-leaf node count
$\eta_{\partial p}$	user access policy includes a number of user attributes
η_{au}	various authorities
$\eta_{\upsilon p}$	in an ordered binary decision diagram, the number of viable paths
Ł_S	length of the element in group G_S
Ł_T	length of the element in group G_T
t_e	duration of a single exponentiation operation
t_p	length of time for a single pairing operation

Table 6: Computation Performance Cost [8].

Scheme	Access Structure	Computation Cost	
		Encryption	Decryption
CPABE (32)	LSSS	(3ηι) te + (2ηι + 1)	te
HABE	LSSS	(4ηι + 1) te + tp	(3η∂ + 1) tp + (η∂) te

Table 7: Performance Of CPABE and HABE's Storage and Communication Costs [8].

Scheme	Access Structure	Storage Cost		Communication cost
		Public key size	Secret key size	Ciphertext size
CPABE (32)	LSSS	$(2\eta_{UA})\ \text{Ł}_S+(\eta_{UA})\ \text{Ł}_T$	$(\eta_{\partial})\ \text{Ł}_S$	$(2\eta_{\iota})\ \text{Ł}_S + (\eta_{\iota} + 1)\ \text{Ł}_T$
HABE (31)	LSSS	$(2\eta_{UA} + 1)\ \text{Ł}_S+\text{Ł}_T$	$(\eta_{\partial} + 2)\ \text{Ł}_S$	$(3\eta_{\iota} + 1)\ \text{Ł}_S + \text{Ł}_T$

that research related to HABE will be more focused on the development of HABE in improving support for revocation mechanisms.

Acknowledgements

This study received support from Doctoral Program of Information System, School of Postgraduate Studies, Universitas Diponegoro

References

[1] Derbisz J. Methods of encrypting monotonic access structures. Ann UMCS Inform. 2011 Jan 1;11(2). https://doi.org/10.2478/v10065-011-0011-x.

[2] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures. In: Proceedings of the 14th ACM conference on Computer and communications security. Alexandria Virginia USA: ACM; 2007. p. 195–203.

[3] Rimal BP, Choi E, Lumb I. A Taxonomy and Survey of Cloud Computing Systems. In: 2009 Fifth International Joint Conference on INC, IMS and IDC. Seoul, South Korea: IEEE; 2009. p. 44–51. https://doi.org/10.1109/NCM.2009.218.

[4] Takabi H, Joshi JB, Ahn GJ. Security and Privacy Challenges in Cloud Computing Environments. IEEE Secur Priv. 2010 Nov;8(6):24–31.

[5] Wu J, Ping L, Ge X, Wang Y, Fu J. Cloud Storage as the Infrastructure of Cloud Computing. In: 2010 International Conference on Intelligent Computing and Cognitive Informatics. Kuala Lumpur, Malaysia: IEEE; 2010. p. 380–3.

[6] Khan AR. ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT. 2012;7(5).

[7] Kamara S, Lauter K. Cryptographic Cloud Storage. In: Sion R, Curtmola R, Dietrich S, Kiayias A, Miret JM, Sako K, et al., editors. Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010. pp. 136–49.

[8] P PK. P SK, P.J.A. A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. J Netw Comput Appl. 2018 Apr;108:37–52.

[9] Chaudhari N, Saini M, Kumar A, Priya G. A Review on Attribute Based Encryption. In: 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN). Tehri, India: IEEE; 2016. p. 380–5. https://doi.org/10.1109/CICN.2016.81.

[10] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy Attribute-Based Encryption. In: 2007 IEEE Symposium on Security and Privacy (SP '07). Berkeley, CA: IEEE; 2007 [cited 2023 Aug 22]. p. 321–34.

[11] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proceedings of the 14th ACM conference on Computer and communications security. Alexandria Virginia USA: ACM; 2007. p. 456–65.

[12] Goyal V, Jain A, Pandey O, Sahai A. Bounded Ciphertext Policy Attribute Based Encryption. In: Aceto L, Damgård I, Goldberg LA, Halldórsson MM, Ingólfsdóttir A, Walukiewicz I, editors. Automata, Languages and Programming. Berlin, Heidelberg: Springer Berlin Heidelberg; 2008. pp. 579–91.

[13] Liang X, Cao Z, Lin H, Xing D. Provably secure and efficient bounded ciphertext policy attribute based encryption. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney Australia: ACM; 2009. p. 343–52.

[14] Waters B. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization. In: Catalano D, Fazio N, Gennaro R, Nicolosi A, editors. Public Key Cryptography – PKC 2011. Berlin, Heidelberg: Springer Berlin Heidelberg; 2011. pp. 53–70.

[15] Li J, Huang Q, Chen X, Chow SS, Wong DS, Xie D. Multi-authority ciphertext-policy attribute-based encryption with accountability. In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. Hong Kong China: ACM; 2011. p. 386–90.

[16] Li J, Wang Q, Wang C, Ren K. Enhancing Attribute-Based Encryption with Attribute Hierarchy. Mob Netw Appl. 2011 Oct;16(5):553–61.

[17] MULTI-AUTHORITY ACCESS CONTROL SYSTEM IN PUBLIC CLOUD STORAGE. Int J Adv Eng. Res Dev. 2017 Nov;4(11).

[18] Nishide T, Yoneyama K, Ohta K. Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures. In: Bellovin SM, Gennaro R, Keromytis A, Yung M, editors. Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg; 2008. pp. 111–29.

[19] Phuong TV, Yang G, Susilo W. Hidden Ciphertext Policy Attribute-Based Encryption Under Standard Assumptions. IEEE Trans Inf Forensics Security. 2016 Jan;11(1):35–45.

[20] Li J, Ren K, Zhu B, Wan Z. Privacy-Aware Attribute-Based Encryption with User Accountability. In: Samarati P, Yung M, Martinelli F, Ardagna CA, editors. Information Security. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009. pp. 347–62.

[21] Lai J, Deng RH, Li Y. Fully Secure Cipertext-Policy Hiding CP-ABE. In: Bao F, Weng J, editors. Information Security Practice and Experience. Berlin, Heidelberg: Springer Berlin Heidelberg; 2011. pp. 24–39.

[22] Jin C, Feng X, Shen Q. Fully Secure Hidden Ciphertext Policy Attribute-Based Encryption with Short Ciphertext Size. In: Proceedings of the 6th International Conference on Communication and Network Security. Singapore Singapore: ACM; 2016. p. 91–8.

[23] Liang X, Cao Z, Lin H, Shao J. Attribute based proxy re-encryption with delegating capabilities. In: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney Australia: ACM; 2009. p. 276–86.

[24] Luo S, Hu J, Chen Z. Ciphertext Policy Attribute-Based Proxy Re-encryption. https://doi.org/10.1007/978-3-642-17650-0_28.

[25] Seo HJ, Kim HW. Attribute-based Proxy Re-encryption with a Constant Number of Pairing Operations. J Inf Commun Converg Eng. 2012 Mar;10(1):53–60.

[26] Li K. Matrix Access structure Policy used in Attribute-Based Proxy Re-encryption.

[27] Liang K, Au MH, Liu JK, Susilo W, Wong DS, Yang G, et al. A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing. Future Gener Comput Syst. 2015 Nov;52:95–108.

[28] Li J, Wang Q, Wang C, Ren K. Enhancing Attribute-Based Encryption with Attribute Hierarchy. https://doi.org/10.1109/CHINACOM.2009.5339938.

[29] Wang S, Zhou J, Liu JK, Yu J, Chen J, Xie W. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. IEEE Trans Inf Forensics Security. 2016 Jun;11(6):1265–77.

[30] Wan Z, Liu J, Deng RH. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing. IEEE Trans Inf Forensics Security. 2012 Apr;7(2):743–54.

[31] Deng H, Wu Q, Qin B, Domingo-Ferrer J, Zhang L, Liu J, et al. Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Inf Sci. 2014 Aug;275:370–84.

[32] Xiao M, Wang M, Liu X, Sun J. Efficient distributed access control for big data in clouds. In: 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Hong Kong, Hong Kong: IEEE; 2015. p. 202–7.