A Novel Monarch Butterfly Optimization with Attribute based Encryption for Secure Public Cloud Storage

G Nagarajan

[1]Assistant Professor & Research Scholar, School of Computing Science and Engineering,
Galgotias University, Greater Noida, Uttar Pradesh
nagarajanite@gmail.com

Dr. K Sampath Kumar

[2] Professor, School of Computing Science and Engineering
Galgotias University, Greater Noida, Uttar Pradesh
ksampathkumara@gmail.com

Abstract - Cloud computing (CC) technology offers proficient exploitation of existing physical resources via virtualization where diverse users share the similar fundamental physical hardware infrastructure. Using the concepts of CC, a set of distributed, scalable, and elastic computing resources are supplied to client through the high-speed Internet. Conventional public key encryption techniques are employed to accomplish data confidentiality, but it could not result in better data sharing. At the same time, attribute-based encryption (ABE) is developed as a significant method in achieving security and establish effective data communication in a simultaneous way. The ABE is a familiar cryptographic technique employed to save the user privacy data in CC. But it is not possible to use in cloud storage because of the computational complexity and decryption key leakage issue. Therefore, this paper presents a novel monarch butterfly optimization with attribute based encryption (MBO-ABE) technique for secure public cloud storage. The presented MBO-ABE technique aims to securely store the data in public cloud storage. ABE purposes to strengthen sensitive data secret in public cloud storage. For improving the security performance of the ABE technique, the MBO manner is applied to it which is based on the migration of monarch butterflies. A wide range of simulations are carried out to highlight the enhanced efficiency of presented MBO-ABE technique. The experimental values showcased that the MBO-ABE technique pointed out the maximum performance of the MBO-ABE technique over the recent state of art methods.

Keywords: Attribute based encryption, Public cloud, security, Monarch butterfly optimization, Optimal key generation

1. Introduction

In recent years, cloud technologies are extensively utilized in several frameworks, services with additional techniques, and several software design methods [1, 2]. The cloud service method comprises infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Framework solutions for the private, public, hybrid, and community schemes based on 4 cloud platform deployment modules [3]. Benefits of CC include accessibility, capacity, and flexibility when connected to the conventional online computing or storage technique. But, the number of security concern is related to the computation cloud include (i) customer related security problems and (ii) security and privacy problems with cloud service providers (CSP) [4]. In the survey, several kinds of attacks interrelated to the power of AES (advanced encryption standard) method is projected such as distinct fault analysis attacks and present faults to the AES framework with the target to retrieve the confidential data [5]. Moreover, CC method could suggest few possible practices of service area, via computation resources for outstanding efficiency in social networking, telecommunication services, web services, and computing applications. Consequently, cloud data centers should contain few methods that are able to guarantee integrity of data and storage perfection that are kept on cloud [6]. Fig. 1 shows the overview of security in CC environment.

Present security system employs more than one attribute immediately, that is, lower security and more time utilization for encrypting or decrypting the data. It creates the procedure more time-consuming and hence rises delays in the network, network use, and power consumption [7]. Hence, this is the accountability of the CSP to give security with each attribute, for example, time consumption, less power consumption, and delay of network. Previously, conventionally available approaches aren't capable of quantifying the security of cloud services efficiently. This architecture must utilize time, lower power, decryption that improve the security of data in CC and delay network utilization with encryption.

Attribute-based encryption (ABE) is a common cryptographic method for protecting the security of user's data in CC. CC is most main areas due to its higher level features like cost saving, convenience, and scalability. Because of its susceptibility, the growth of the security method is highly complex. Thus, the availability and economic benefit would be influenced [8]. The attacker creates the attack in devices and mobile applications in that place to improve the hypervisor for destroying the DOS and VM side channel attacks. The CC would be influenced by the existence of traffic, where the case IP address is utilized for eliminating the traffic. A method such as privacy preserving is utilized for allowing public auditing via this manner. The shared information has an amount of blocks comprising the signer identity and the data are retained confidential from 3rd party till the authentication of shared data.

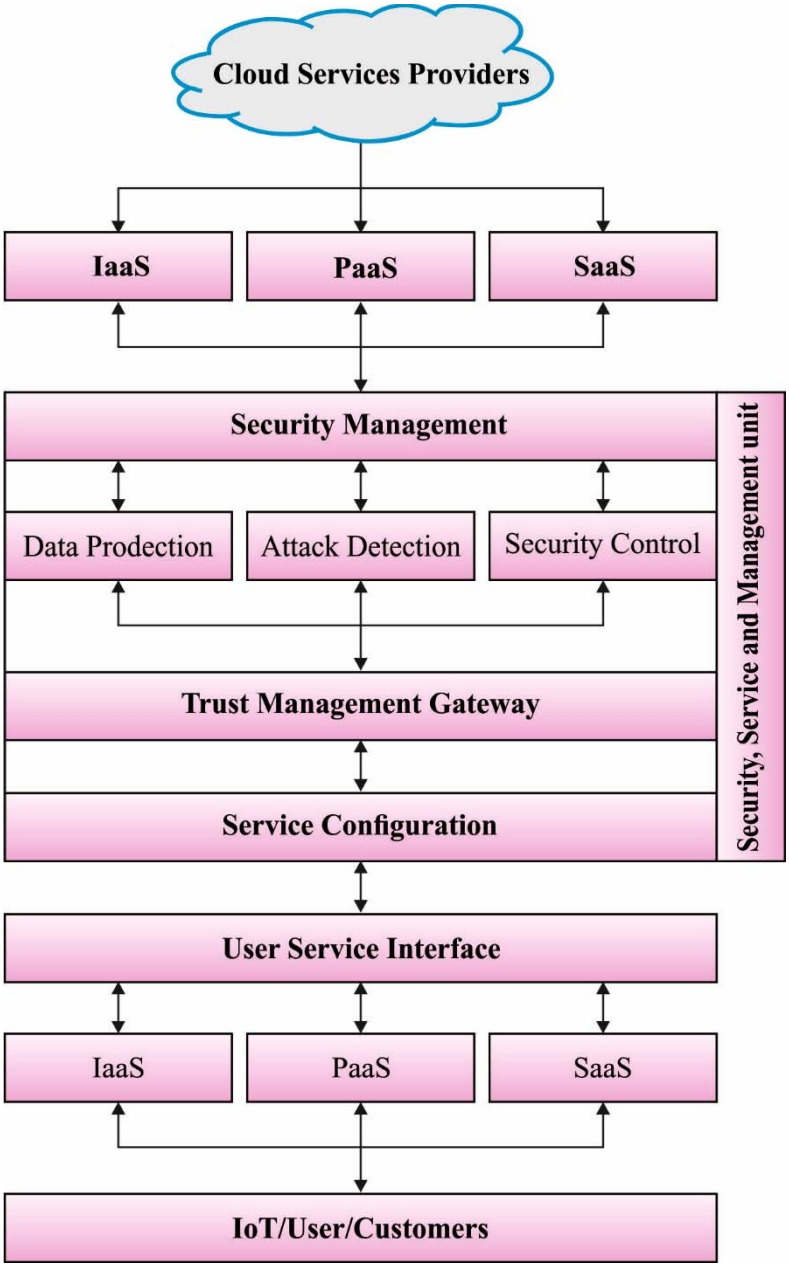

Fig. 1. Overview of security in CC environment

This paper presents a novel monarch butterfly optimization with attribute based encryption (MBO-ABE) technique for secure public cloud storage. The proposed MBO-ABE technique intends to secure storage of data in the public cloud storage in order to strengthen sensitive data confidentiality. For boosting the security outcomes of the ABE technique, the MBO algorithm is applied to it which is based on the migration of monarch butterflies. An extensive set of experimental analyses take place to guarantee the betterment of the proposed MBO-ABE technique.

2. Literature Review

This section reviews the state of art encryption techniques developed for cloud environments. Prathap and Mohanasundaram [9] offered a 2 side decryption method which could be decrypted using 2 entities (i.e., receiver and centralized authentication agent) therefore enhancing the message passing security by permitting the central authentication agent for reading the transmitting words. Deng et al. [10] formalized and introduced an IBET module by easily incorporating 2 traditional encryption methods, such as IBE and IBBE. In IBET, data user is authorized and identified for accessing data on the basis of their recognisable identities that evades complex certificate management in normal secure distributed schemes. Fun et al. [11] expanded the Honey Encryption system for enhancing the file storage security on the public CC. The Honey Encryption offers the encrypted data a further protection layer by offering fake data regarding each wrong presumption on the users' passwords. Such fake data resembles the actual data and indistinguishable from the attacker's viewpoint, thus harden the difficulty of password predicting.

Shen et al. [12] presented a system for a multi security level cloud storage scheme i.e., integrated by the AES symmetric encryption and an enhanced identity based PRE method. Liu [13] proposed a few techniques of creating secure public key encryption system against interrelated arbitrariness attacks, viz., RRA-CPA secure public key encryption system using effective decryption method and short ciphertext size. Veeraragavan et al. [14] proposed an EEA to secure the data in cloud storage. It utilizes similar key for decrypting and encrypting the data beforehand saved in to the cloud. Results of the projected EEA generated distinct ciphertext for similar plaintext. Krishnasamy and Venkatachalam [15] utilized a secure AP3DE method for verifying with confidence expertise of aggregate technology.

3. Preliminaries

3.1. CP-ABE

The CP-ABE model encompasses KGC, encryption, and decryption. The KGC problems confidential key based on user attribute. The encryption encrypts the message based on elected access policies. The decryption is decrypted the ciphertext effectively only if their attribute fulfills the equivalent access policy. There are 4 techniques in CP-ABE model:

1) Setup: it gets security parameters as input as well as output public variables PP and master secret key MSK.
2) Key_Gen: it gets PP, MSK, and the group of attributes S as input as well as output secret key SEK_{S} equivalent to S.
3) Encryption: it gets PP, access policies $\mathbb{W}$, and message Mes as input as well as output the ciphertext $CT_{\mathbb{W}}$.
4) Decryption: it gets PP, $CT_{\mathbb{W}}$, and SK_{S} as input and output the message Mes, if and only if the attribute S fulfill the $\mathbb{W}$; for instance, $S \vDash \mathbb{W}$.

3.2. Oblivious Transfer (OT)

The OT protocols are 2-party calculation protocols in that one party is the sending side ($\mathcal{S}$) and the remaining one is recipients ($\mathcal{R}$). The protocol makes sure the subsequent: $\mathcal{S}$ send the set of messages to $\mathcal{R}$. $\mathcal{R}$ obtains the division of these messages, however, $\mathcal{S}$ doesn't identify that message as $\mathcal{R}$ received. It can be drawn on a classic (OT_2^1) protocols [16]:

(1) $\mathcal{R}$ arbitrarily selects $\alpha, \beta, \gamma \in [1, q]$ and sets τ as follows:

(a) If $\sigma = 0$, then $\tau = \left(g^{\alpha}, g^{\beta}, g^{\alpha\beta}, g^{\gamma}\right)$.

(b) If $\sigma = 1$, then $\tau = \left(g^{\alpha}, g^{\beta}, g^{\gamma}, g^{\alpha\beta}\right)$.

$\mathcal{R}$ sends τ to $\mathcal{S}$.

(2) $\mathcal{S}$ receives $= (\mathrm{x}, y, z_0, z_1)$. Afterward, $\mathcal{S}$ verifies $z_0 \neq z_1$. If not, its output $\perp$, and abort.

Also, $\mathcal{S}$ selects $u_0, u_1, V_0, V_1 \in [1, q]$ arbitrarily and calculates the following 4 values:

$$\omega_0 = x^{u_0} \cdot g^{v_0},$$

$$k_0 = (z_0)^{u_0} \cdot y^{v_0} \quad (1)$$

$$\omega_1 = x^{u_1} \cdot g^{v_1},$$

$$k_1 = (z_1)^{u_1} \cdot y^{v_1}$$

Afterward, $\mathcal{S}$ computes $\mathrm{c}_0 = \mathrm{x}_0 \cdot k_0, c_1 = x_1 \cdot k_1$ and sends (ω_0, c_0) and (ω_1, c_1) to $\mathcal{R}$. Eventually, $\mathcal{R}$ computes $k_\sigma = (\omega_0)^\beta$ and attains $\delta_\sigma = c_\sigma \cdot (k_\sigma)^{-1}$

3.3. Bilinear Maps

Assume that $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be 3 q order cyclic group. The bilinear pairing function e is a bilinear map, $:\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, and fulfills the following properties:

(1) $\forall g \in \mathbb{G}_1,\ \forall h \in \mathbb{G}_2,\ \forall x, y \in Z_q^*,$ there is $e(g^x, h^y) = e(g,h)^{xy}(2)\exists g_0 \in \mathbb{G}_1,\ \exists h_0 \in \mathbb{G}_2,\ e(g_0, h_0) \neq 1(3)\forall g \in \mathbb{G}_1, \forall h \in \mathbb{G}_2, e(g,h)$ is estimated in polynomial time

It is utilized asymmetric bilinear groups; i.e, $\mathbb{G}_1 \neq \mathbb{G}_2$.

3.4. Security Assumption

Definition 1. Assume that $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ procedure bilinear group, assume g be a generator of $\mathbb{G}_1$, and consider h be generator of $\mathbb{G}_2$. In order to few unknown $\alpha \in \mathbb{Z}_p^*$, determine $g_i = g^{\alpha^i}$, and set $\vec{y}_{g,\alpha,n} = (g_1, \ldots, g_n, g_{n+2}, \ldots, g_{2n})$. It is approximately a technique $\mathcal{B}$ resolves *n*- BDHE issue with benefit ϵ if on input g, $h, \vec{y}_{g,\alpha,n}$,

$$|\Pr|\left[\mathcal{B}\left(e(\mathrm{g}_{n+1}, h)\right) = 1\right] - \Pr[\mathcal{B}(Z) = 1] \geq \epsilon, \qquad (2)$$

where Z implies the arbitrary element of $\mathbb{G}_T^*$.

4. The Proposed MBO-ABE Technique

In the proposed model, users submit their attributes and important suggestion to AAC. Fig. 2 shows the basic model of the proposed MBO-ABE technique. For practical uses, AAC is frequently performed as the institution which gives certification to user attribute like government office, as it identifies the attribute of user itself and does not cause further leak. This token doesn't expose that some data of user attributes and only make sure the authenticities. If the user requires for obtaining their attribute key, it is submitting the blind token to KGC that is technical institutions. Afterward, the user attains the blind keys, it removes the confidential key locally. The particular procedure is as follows:

i. The client illustrates their attribute and significant evidence to AAC.
ii. The AAC check the user attribute as well as return a blind token to user with their signatures.
iii. If the user requires for obtaining their attribute key, it is to submitted its blind token to KGC. The KGC could not reach some data on the user attribute. It only authorizes that the user's truly is compared attribute.
iv. The KGC initial check the legitimacy of tokens, and when the signature is illegals, it aborts; and then, it run the key generation technique and outcomes a blind key.
v. The client obtains the blind key to KGC and removes the private key.

ABE is a popular cryptographic technology for protecting the security of user data in CC. The multi-authority CP-ABE scheme with identity based user revocation is included as following techniques [17]:

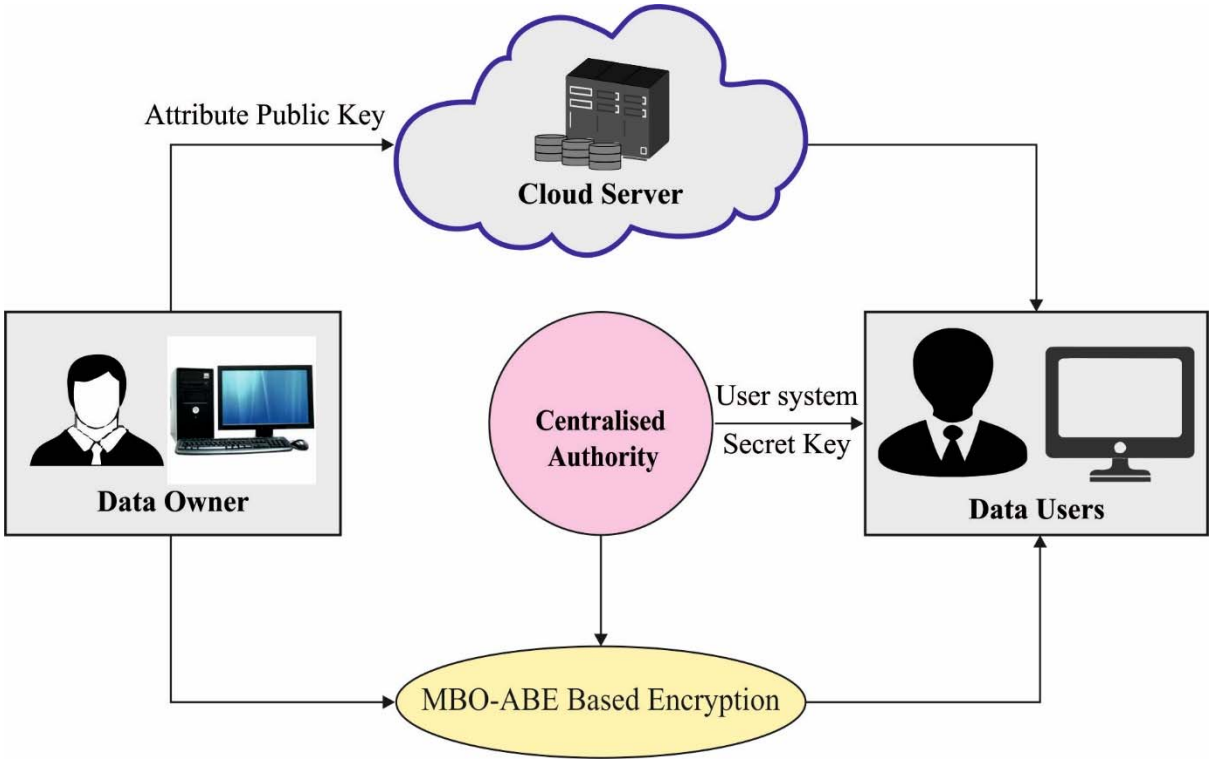

Fig. 2. Overall process of proposed model

Global Setup $(\lambda) \rightarrow GLP$. The global setup technique gets in security parameters λ and output global parameter GLP for model.

Central Authority Setup $(GLP) \rightarrow (SEK*, PUK^*)$. A central authority run this technique with GLP as input for producing their individual secret key and public key pairs are SEK^*, PUK^*

Identity KeyGen $(GLP, RL, GID) \rightarrow K^*_{GID}$. The central authority runs this technique up on user requests to identity secret keys. It forms if the request is effective and when yes, creates K^*_{GID}.

Authority Setup $(GLP) \rightarrow (PUK, SEK)$. All attributes authority run the authority setup technique with GP as input for producing their individual secret key and public key pairs are SEK, PUK.

KeyGen $(GLP, SEK, GID, i) \rightarrow K_{i,GID}$. The attribute key generation technique gets in an identity GID, the global parameter, an attribute i going to few authorities, and the secret key SEK for this authority. It makes a key $K_{i,GID}$ for this attribute, identity pair.

Encrypt (GLP, $\mathcal{M}es$, (A, ρ), $\{PUK\}$, PUK^*, $RL) \rightarrow CT$. The encrypted technique takes in message $\mathcal{M}es$, an access matrix (A, ρ), the group of public keys for significant authority, the public key of central authorities, the revoked users list, and global parameter. It output a ciphertext CT.

Decrypt (GLP, CT, (A, ρ), $\{K_{i,GID}\}$, K^*_{GID}, $RL) \rightarrow \mathcal{M}es$. The decrypted technique take in global parameter, the revoked user lists, the CT, identity key and the gathered of keys equivalent to attributes, identity pair every with the similar stable identity GID. It output either the message $\mathcal{M}es$ if the gathered of attributes i fulfills the access matrix equivalent to CT. Then, decrypted fails.

For improving the performance of the ABE technique, the MBO technique is introduced. The MBO technique is a population based technique that is regarded as go to the type of SI techniques that are simulated as performance of particular species with swarm tendencies. As noted previously, the MBO is presented Wang et al. [18], based its idea for this smart technique on a type of butterflies that is native to North America and that is considered as the beauty of their procedure that has orange and black colors. The migratory performance of these butterflies is inspired for solving different optimization issues. In many rules and fundamental models which is observed for attaining the optimum solution to issues:

1. Every butterfly which creates the population is also present in L_1 (home earlier to migrate) or L_2 (home next to migrate).
2. All children of every butterfly were created with migration function, regardless of if the parents are

existed in L_1 or L_2.

3. The population must not alter and must be ever constant, therefore 2 (either the novel child or the parent) is eliminated with FF.
4. The butterflies that are elected dependent upon FF are accepted to the next generation and are not altered with migration function.

A migrate function of butterflies is written as:

$$X_{i,j}^{t+1} = X_{r1.k}^{t} \tag{3}$$

where $X_{i,j}^{t+1}$ implies the *K*th element of *Xi at* $t+1$ generation that expressed the place of butterflies i, and $X_{r1.k}^{t}$ implies the *K*th element of novel generation place. At this point, r represents the arbitrary number computed as formula:

$$R = rand * peri \tag{4}$$

Where $peri$ stands for the migration period time [19].

Conversely, if $r >$ p, after the *K*th element of novel generation place are computed as formula:

$$X_{i,j}^{t+1} = X_{r2.k}^{t} \tag{5}$$

Where $X_{r2.k}^{t}$ denotes the K^{th} element of *Xr*2 at t generation of butterfly *r*2. So that *P* demonstrates the ratio of monarch butterfly in L_1.

Butterfly adjustment operator aims to balance amongst the way of migration from L_1 to L_2 is attained by changing the ratio of *P* value. When the value of *P* is huge, it implies that the amount of butterflies is elected from L_1 is superior to L_2, and equally.

The place of butterfly is adjusting when the created rand is lesser or equivalent to the value of P. The following formula showcases the upgraded place of butterflies place:

$$X_{j.k}^{t+1} = X_{best.k}^{t} \tag{6}$$

Where $X_{j.k}^{t+1}$ signifies the K^{th} element of *Xj* at $t+1$ generation that expressed the butterflies j place, and $X_{best.k}^{t}$ implies the K^{th} element of *Xbest* at present generation t in both L_1 and L_2. At this point, when $rand > P$, afterward, it can be upgraded as formula:

$$X_{i,j}^{t+1} = X_{r3.k}^{t} \tag{7}$$

Conversely, when $rand$ implies the superior to BAR, the novel place was upgraded as formula:

$$X_{j.k}^{t+1} = X_{j.k}^{t+1} + \alpha * (dx_k - 0.5) \tag{8}$$

Where BAR signifies the alteration rate of butterflies and dx refers to the walk step of j butterflies that is computed as carrying out Lévy flight as:

$$(Dx = Lévy(X_j^t) \tag{9}$$

α in Eq. (8) denotes the weighted factor which is estimated as formula:

$$\alpha = S_{\max} = t^2 \tag{10}$$

Where $S_{\max}$ demonstrates the max length of butterflies walk in one step and t refers the present generations. Fig. 3 demonstrates the flowchart of MBO.

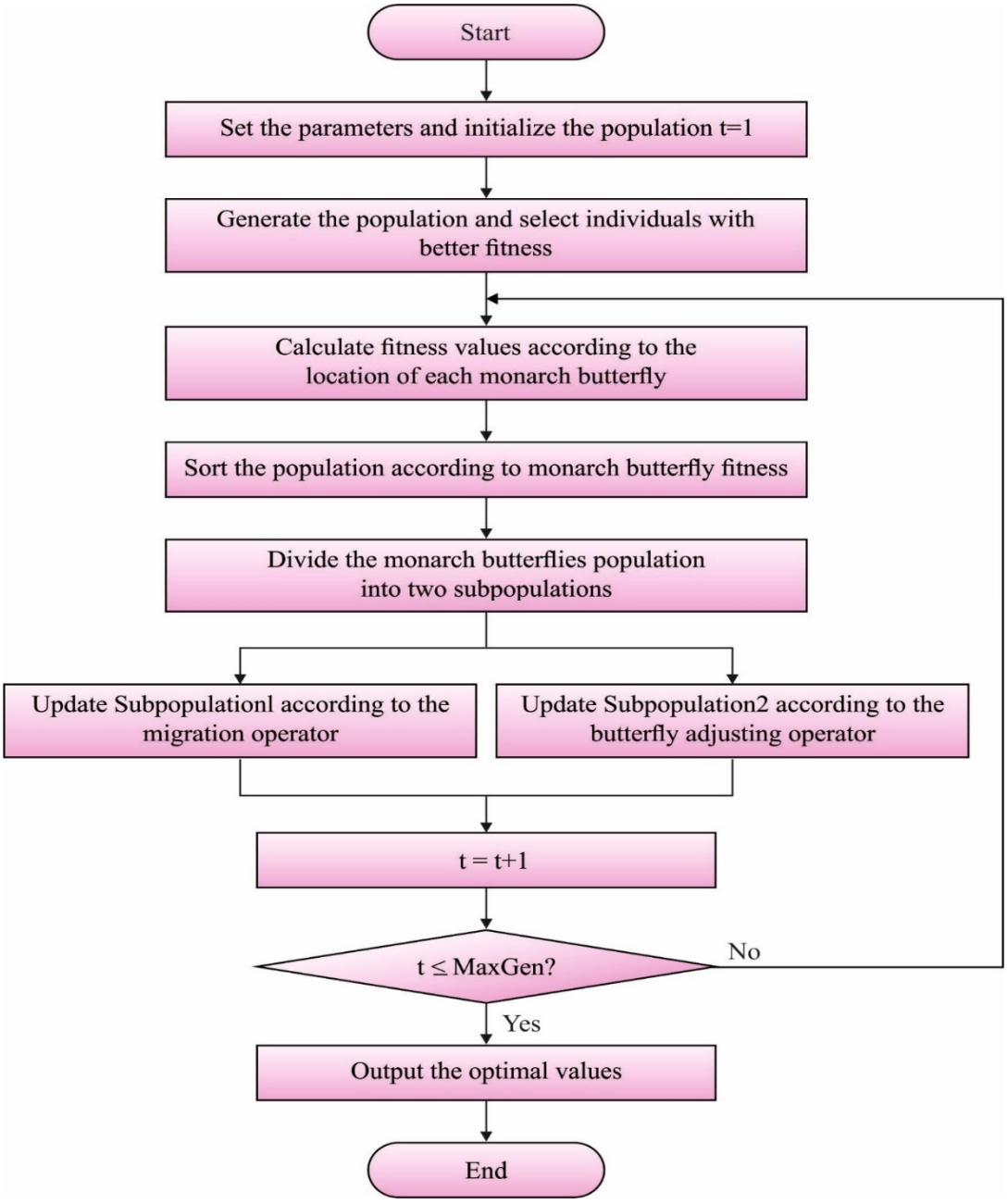

Fig. 3. Flowchart of MBO algorithm

5. Performance Validation

This section examines the performance of the proposed MBO-ABE technique with respect to several dimensions. Table 1 showcases the encryption and decryption time analysis of the proposed MBO-ABE technique under varying file sizes. A throughput analysis demonstrated that the MBO-ABE technique has gained maximum throughput of 0.00952, 0.00943, and 0.00932 for the file sizes of 1-3GB respectively.

Table 1 Result analysis of MBO-ABE model in terms of Encryption and Decryption time

Encryption Time (sec)			
File Size (GB)	**MBO-ABE**	**BH-WABE**	**HABE**
1	105	118	132
2	212	230	250
3	322	341	362
Decryption Time (sec)			
File Size (GB)	**MBO-ABE**	**BH-WABE**	**HABE**
1	102	113	123
2	200	221	262
3	524	598	625
Throughput			
File Size (GB)	**MBO-ABE**	**BH-WABE**	**HABE**
1	0.00952	0.00847	0.00758
2	0.00943	0.00869	0.00800
3	0.00932	0.00874	0.00828

Fig. 4 depicts the encryption time analysis of the MBO-ABE technique with other algorithms under three file sizes. The figure portrayed that the MBO-ABE technique requires lower encryption tome over the other techniques. For instance, with the file size of 1GB, the MBO-ABE technique has offered a minimal encryption time of 105s whereas the BH-WABE and HABE techniques have demonstrated a higher encryption time of 118s and 132s respectively. Likewise, with the file size of 3GB, the MBO-ABE method has offered a minimum encryption time of 322s whereas the BH-WABE and HABE algorithms have portrayed a superior encryption time of 341s and 362s correspondingly.

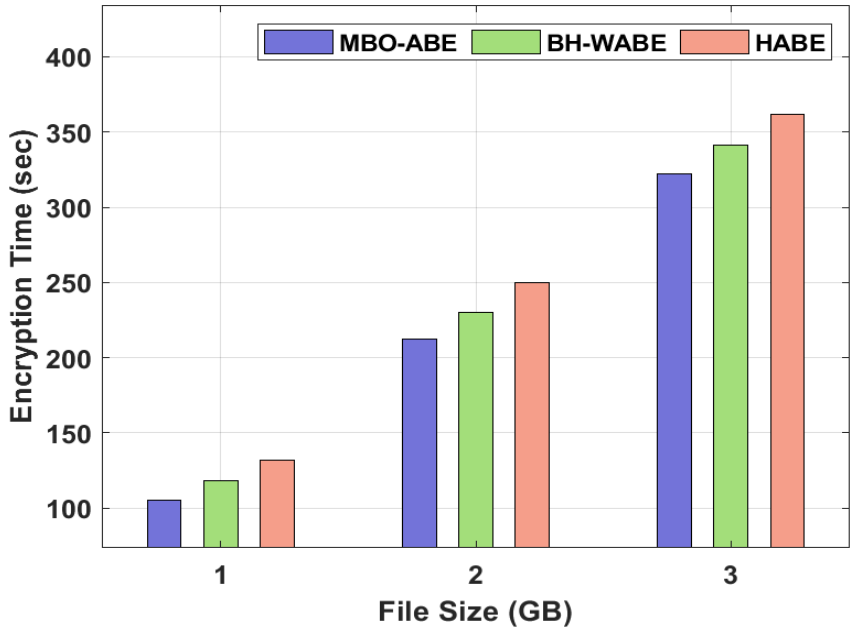

Fig. 4. Encryption time analysis of MBO-ABE model

Fig. 5 demonstrates the decryption time analysis of the MBO-ABE manner with other algorithms under three file sizes. The figure outperformed that the MBO-ABE method needs minimum decryption tome over the other techniques. For sample, with the file size of 1GB, the MBO-ABE technique has offered a lesser decryption time of 102s whereas the BH-WABE and HABE techniques have showcased an improved decryption time of 113s and 123s respectively. Similarly, with the file size of 3GB, the MBO-ABE method has offered a minimal decryption time of 524s whereas the BH-WABE and HABE methodologies have demonstrated a higher decryption time of 598s and 625s correspondingly.

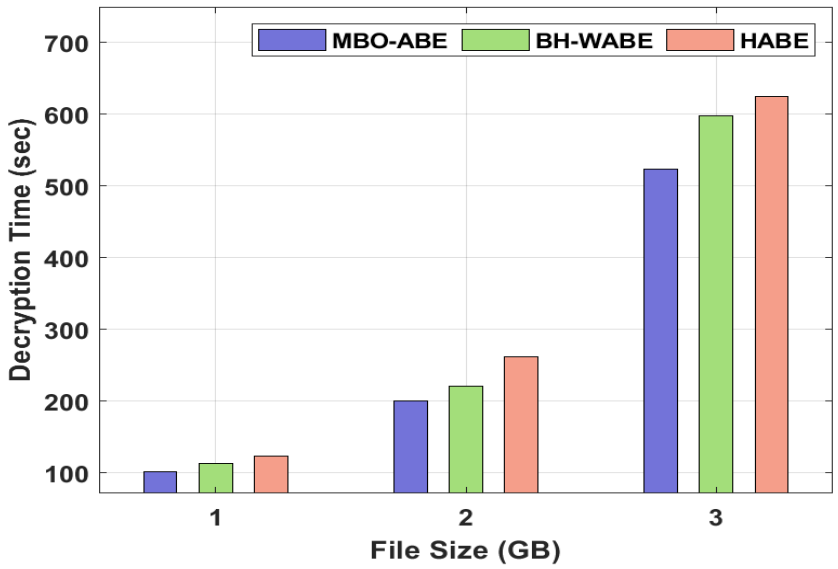

Fig. 5 Decryption time analysis of MBO-ABE model

Table 2 showcases the User key generation time (UKGT) and storage cost of secret key (SCSK) analysis of the presented MBO-ABE manner under varying weighted attributes. Fig. 6 illustrates the UKGT time analysis of the MBO-ABE method with other manners under number of weighted attributes. The figure exhibited that the MBO-ABE approach needs minimum UKGT tome over the other algorithms. For sample, with the weighted attributes of 10, the MBO-ABE manner has offered a lesser UKGT time of 0.63s whereas the BH-WABE and HABE techniques have outperformed a superior UKGT time of 1.00s and 1.50s correspondingly. At the same time, with the weighted attributes of 50, the MBO-ABE technique has offered a minimal UKGT time of 2.39s whereas the BH-WABE and HABE methods have demonstrated a superior UKGT time of 3.50s and 5.50s correspondingly.

Table 2 Result analysis of MBO-ABE model under User key generation and storage-follow encryption time

User Key Generation Time (s)			
Count of Weighted Attributes	**MBO-ABE**	**BH-WABE**	**HABE**
10	0.63	1.00	1.50
20	1.13	1.61	2.50
30	1.67	2.50	3.00
40	1.94	2.80	4.00
50	2.39	3.50	5.50
Storage Cost of Secret Key (KB)			
Count of Weighted Attributes	**MBO-ABE**	**BH-WABE**	**HABE**
10	1	2	3
20	2	3	6
30	3	4	8
40	4	6	10
50	6	8	13

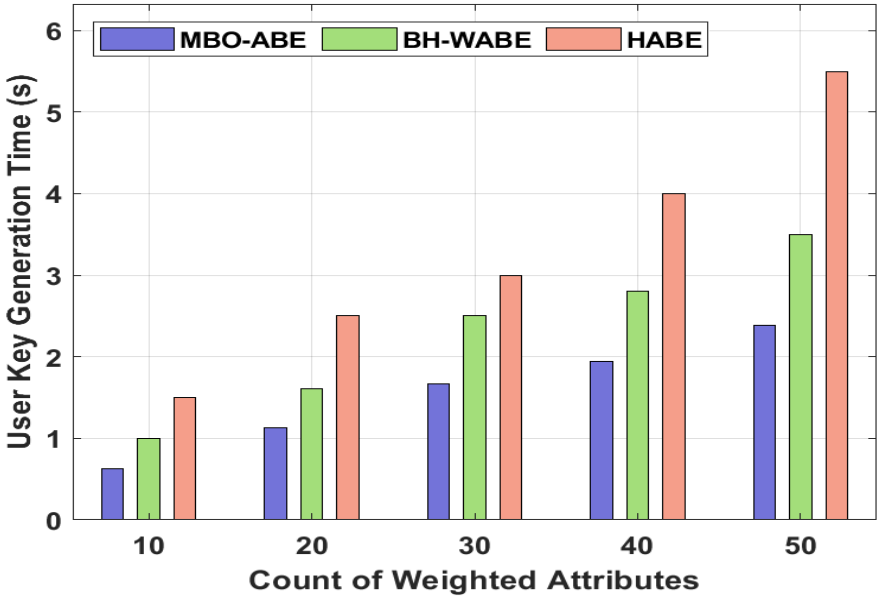

Fig. 6. UKGT analysis of MBO-ABE model

Fig. 7 shows the SCSK time analysis of the MBO-ABE manner with other techniques under number of weighted attributes. The figure demonstrated that the MBO-ABE manner requires lesser SCSK tome over the other techniques. For instance, with the weighted attributes of 10, the MBO-ABE manner has offered a minimum SCSK time of 1KB whereas the BH-WABE and HABE methodologies have exhibited an improved SCSK time of 2KB and 3KB correspondingly. Followed by, with the weighted attributes of 50, the MBO-ABE technique has offered a minimal SCSK time of 6KB whereas the BH-WABE and HABE algorithms have exhibited a maximum SCSK time of 8KB and 13KB correspondingly.

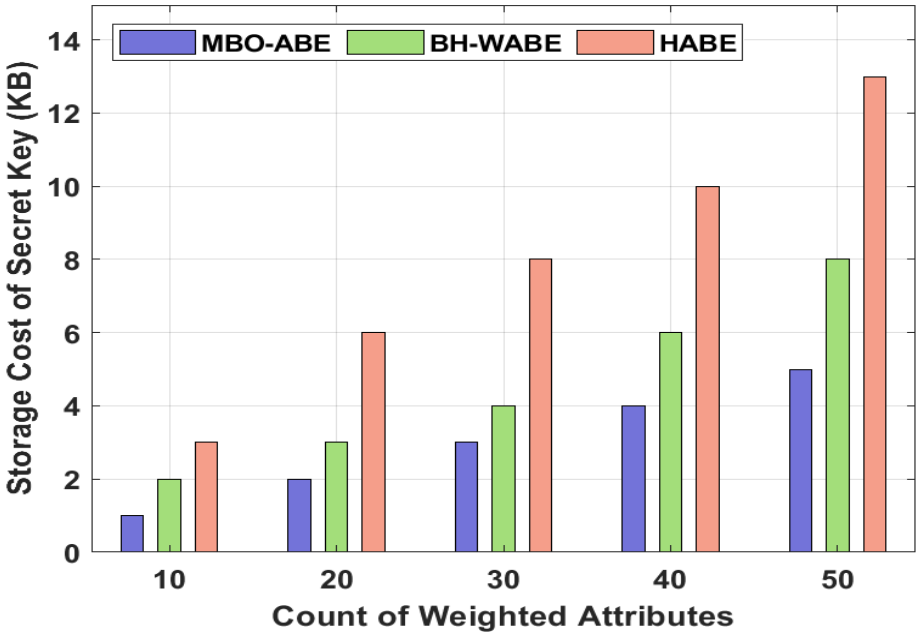

Fig. 7. SCSK analysis of MBO-ABE model

6. Conclusion

This paper has presented a new MBO-ABE technique to achieve security in public cloud storage systems. The proposed MBO-ABE technique intends secure storage of data in the public cloud storage in order to strengthen sensitive data confidentiality. For boosting the security outcomes of the ABE technique, the MBO algorithm is applied to it which is based on the migration of monarch butterflies. For showcasing the improved outcomes of the presented MBO-ABE method, an extensive set of experimental analyses take place. The experimental values

showcased that the MBO-ABE technique pointed out the superior performance of the MBO-ABE technique over the recent state of art methods. In future, light weight authentication and block technologies can be incorporated to accomplish improved security in public cloud storage systems.

References

[1] Awan, I.A., Shiraz, M., Hashmi, M.U., Shaheen, Q., Akhtar, R. and Ditta, A., 2020. Secure framework enhancing AES algorithm in cloud computing. *Security and Communication Networks*, *2020*.
[2] Mahmood, G.S., Huang, D.J. and Jaleel, B.A., 2019. Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing. *Int. J. Netw. Secur.*, *21*(2), pp.326-332.
[3] Othman, S. and Riaz, A.S., 2018. A user-based trust model for cloud computing environment. *International Journal of Advanced Computer Science and Applications*, *9*(3).
[4] Pradeep, K.V., Vijayakumar, V. and Subramaniyaswamy, V., 2019. An efficient framework for sharing a file in a secure manner using asymmetric key distribution management in cloud environment. *Journal of Computer Networks and Communications*, *2019*.
[5] Kpelou, M. and Kishore, K., 2019. Lightweight security framework for data outsourcing and storage in mobile cloud computing. *International Journal of Recent Technology and Engineering*, *8*(2).
[6] Elgendy, I.A., Zhang, W.Z., Liu, C.Y. and Hsu, C.H., 2018. An efficient and secured framework for mobile cloud computing. *IEEE Transactions on Cloud Computing*, *9*(1), pp.79-87.
[7] Saha, R., Geetha, G., Kumar, G. and Kim, T.H., 2018. RK-AES: an improved version of AES using a new key generation process with random keys. *Security and Communication Networks*, *2018*.
[8] Ghosh, S. and Karar, V., 2018. Blowfish hybridized weighted attribute-based encryption for secure and efficient data collaboration in cloud computing. *Applied Sciences*, *8*(7), p.1119.
[9] Prathap, R. and Mohanasundaram, R., 2021. Enhancing security by two-way decryption of message passing of EMR in public cloud. International Journal of Intelligent Enterprise, 8(2-3), pp.239-250.
[10] Deng, H., Qin, Z., Wu, Q., Guan, Z., Deng, R.H., Wang, Y. and Zhou, Y., 2020. Identity-based encryption transformation for flexible sharing of encrypted data in public cloud. IEEE Transactions on Information Forensics and Security, 15, pp.3168--3180.
[11] Fun, T.S., Samsudin, A. and Zaaba, Z.F., 2017. Enhanced security for public cloud storage with honey encryption. Advanced Science Letters, 23(5), pp.4232-4235.
[12] Shen, J., Deng, X. and Xu, Z., 2019. Multi-security-level cloud storage system based on improved proxy re-encryption. EURASIP Journal on Wireless Communications and Networking, 2019(1), pp.1-12.
[13] Liu, P., 2020. Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/edge computing. IEEE Access, 8, pp.16750-16759.
[14] Veeraragavan, N., Arockiam, L. and Manikandasaran, S.S., 2017, February. Enhanced encryption algorithm (EEA) for protecting users' credentials in public cloud. In 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) (pp. 1-6). IEEE.
[15] Krishnasamy, V. and Venkatachalam, S., 2021. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings.
[16] Song, Y., Wang, H., Wei, X. and Wu, L., 2019. Efficient attribute-based encryption with privacy-preserving key generation and its application in industrial cloud. *Security and Communication Networks*, *2019*.
[17] Horváth, M., 2015, January. Attribute-based encryption optimized for cloud computing. In *International Conference on Current Trends in Theory and Practice of Informatics* (pp. 566-577). Springer, Berlin, Heidelberg.
[18] Feng, Y., Yang, J., Wu, C., Lu, M. and Zhao, X.J., 2018. Solving 0–1 knapsack problems by chaotic monarch butterfly optimization algorithm with Gaussian mutation. *Memetic Computing*, *10*(2), pp.135-150.
[19] Alweshah, M., Al Khalaileh, S., Gupta, B.B., Almomani, A., Hammouri, A.I. and Al-Betar, M.A., 2020. The monarch butterfly optimization algorithm for solving feature selection problems. *Neural Computing and Applications*, pp.1-15.
[20] Nagarajan, G. and Sampath Kumar, K., 2021. Security Threats and Challenges in Public Cloud Storage. *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*.
[21] Nagarajan, G. (2021). Comparative Analysis of Public Cloud Security Based Schemes and Cryptographic Algorithms. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(13), 2114-2127.