Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.018580
Article

Tech Science Press

TAR-AFT: A Framework to Secure Shared Cloud Data with Group Management

K. Ambika[1,*] and M. Balasingh Moses[2]

[1]Department of Computer Science Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, India
[2]Department of Electrical and Electronics Engineering, University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, India
*Corresponding Author: K. Ambika. Email: ambimahesh4033@gmail.com

Received: 12 March 2021; Accepted: 15 June 2021

Abstract: In addition to replacing desktop-based methods, cloud computing is playing a significant role in several areas of data management. The health care industry, where so much data is needed to be handled correctly, is another arena in which artificial intelligence has a big role to play. The upshot of this innovation led to the creation of multiple healthcare clouds. The challenge of data privacy and confidentiality is the same for different clouds. Many existing works has provided security framework to ensure the security of data in clouds but still the drawback on revocation, resisting collusion attack along with privacy of data present a complex problem. For preserving the data privacy and confidentiality, a novel framework is proposed with two novel algorithms of Threat Aware Revocation (TAR) and Advance Flexi Twister Secret Block Encryption Standard (AFT-SBES) both are named as TAR-AFT. The TAR algorithm is mainly focus on generates the user signature and the AFT-SBES algorithm to generate the key. Both the signature and key are distributed to the users for enhancing the security to access cloud storage and files. The self-session shadow approach is used to monitor the activities of the cloud users. The revocation is carried out through removal of signature from the Enhanced Dynamic Hash Table (EDHT). From the performance analysis of TAR-AFT, it provides more effective to accessing of data stored in cloud and security such as data privacy and confidentiality.

Keywords: Cloud; confidentiality; privacy; user revocation; signature; TAR-AFT

Notations:

TAR	Threat Aware Revocation
AFT-SBES	Advance Flexi Twister Secret Block Encryption Standard
EDHT	Enhanced Dynamic Hash Table
SSS	Self-Session Shadow
N	Maximum Number of Users
P_k	Public Key
M_k	Master Key

G_m	Multiplicative Group
G_{mt}	Squared Multiplicative Group
OD	Owner Details
OID	Owner Identity
A_P	Access Policies
G_a, G_b	Additive Group
G	Generators of The Group
CA	Cloud Authority
SP	Security Parameter
ON	Owner Name
OD	Owner Details
OID	Owner Identity
A_P	Access Policies
UN	User Name
UA	User Attributes
UID	User Identity
UD	Digital Signature of User

1 Introduction

The cloud computing technology is employed in various domains for data management. The cloud computing offers high flexibility, rapid scaling and incurs very low cost [1]. Among the other several domains, the cloud computing is extensively used among the health care domain. The health care domain involves the accumulation of enormous amount of data to form Electronic Health Records (EHR) and it is required for effective data management [2]. In general, the EHR involves the personal data of owner along with their laboratory data and several reports. However, the issue of security in the contemporary cloud environment is prevalent among the health care clouds. In particular, the owner data to be accessed only by authorized person [3] and the confidentiality of their data has to be managed in the health care clouds [4]. The issue of privacy arises in the cloud during sharing of the sensitive information and often it is accessed by the unauthorized persons intentionally or accidentally [5,6]. The confidentiality issues emerges from the misuse of available data for any research activities without the consent from the owner or health care organization and are subjected to legal compliances [7]. The medical personals are the authorized persons in the health care cloud to access the owner data and under some circumstances of information leakage or unsatisfactory treatment, the owner can revoke them. The process of revocation often adds the computation burden in the exiting cloud systems and the revoked user can be a threat over the sensitive information [8].

Several research works are carried out through the development of novel algorithms and it is observed that those single approaches did not provide the necessary cloud data security [9]. The inadequacy of the effective health care system has resulted in several disruptions among the health care industries and limited it progress [10]. The cryptic algorithm-based systems are deployed for securing the owner health data and under any cyber-attacks, the possibility of key leakage is high [11]. The Role Based Access Control (RBAC) techniques are being proposed for ensuring the privacy and confidentiality of owner data through the attribute -based encryptions and access policies are also suspectable to leakage of data and do not address the revocation problems effectively [12,13]. Due to the existing issues, the better security over the owner data can be accomplished through authentication mechanism using digital signature and effective encryption scheme [14].

For preserving the owner privacy and their data confidentiality in the health care cloud, the novel technique proposed through the novel signature generation and key generation technique in the form of Threat Aware Revocation (TAR) and Advance Flexi Twister Secret Block Encryption Standard (AFT-SBES) is being used. The proposed framework uses the secret prime twisting approach to improve the robustness of both the signature and the keys. The proposed framework also helps in effective revocation in the health care cloud.

The novel TAR-AFT framework is developed to ensure the data privacy and confidentiality through the following contributions

- A novel Threat Aware Revocation (TAR) algorithm is proposed for signature generation that regulates the access of owner data in the health care cloud and the revocation is carried out through the nullifying of signature.
- The novel Advance Flexi Twister Secret Block Encryption Standard (AFT-SBES) algorithm is proposed to ensure the privacy and confidentiality of owner data in the cloud.
- The SelfSession Shadow (SSS) is employed to monitor the activities of the group members and support the revocation process.
- The generated key is split into blocks and the generated signature is updated and modified through the secret prime twister algorithm.
- The performance of the propose framework is evaluated over the performance metrics to exhibit the capability in ensuring the data privacy and confidentiality.

The present work is expressed with the following sections: Section 2 involves the related work on clouds. Section 3 deliberates the preliminaries for the framework and Section 4 provides the system architecture and security model. Section 5 list out the algorithms for the proposed framework. Section 6 explains the simulation results along with the discussion and Section 7 provides conclusion and future work.

2 Related Works

Prince et al. is proposed to provide the access control based on privacy rating in order to preserve the data confidentiality and privacy of the cloud health data. The privacy rating is estimated for the data present and user accessing any data in the cloud [15]. Liu et al. proposed signature scheme of Lightweight and Privacy-Preserving Medical Services Access (LPP-MSA) is proposed to secure the data and reduce the computational overhead in the existing attribute-based signature scheme. It additionally accomplished resistant against the collusion attack with anonymity and unforgeability [16].

Afnan et al. An AES is employed to preserve the patient Electronic Health Record (EHR) through the integration of organization-based access control (Or-BAC). It performs two-layer encryption to ensure the confidentiality and security [17]. Omar et al. focus on a patient centric health care system through the block-chain technology to preserve the data privacy. The proposed framework involves the encryption of data along with pseudonymity [18]. Chang et al. framework for ensuring the secure sharing of health care data through the searchable encryption technique and privacy preserving equity test with the addition of message authentication code and bloom filter technique [19]. Sharaf et al. proposed a security framework with ciphertext-attribute based encryption meet the requirements of the health care system for the government organization. It offered fine grained access control over the multiple authorities that facilitate the communication among both citizen and government. The multifactor authentication for applicants is established and validated through two authorities [20]. Mayank et al. focused a hybrid technique is proposed with k-anonymity and size restricted query set to ensure the confidentiality of health care data from inference attacks and linking attacks. The rule set is developed to improve the privacy of data through both techniques [21].

Azath et al. proposed Attribute based health record protection scheme for securing the data is established to reduce the administrational and computational load on health care system. The proposed scheme involved access control and privilege mode to encrypt the information and authenticate the message respectively to preserve the data [22]. Kashish et al. proposed biometric authentication approach for securing the cloud health data was proposed through the neural network and named it as BAM HealthCloud. The proposed scheme overcomes the issue of forgetting password and token theft [23]. Kirit et al. proposed novel hybrid approach is proposed with ElGamal cryptography-based re-encryption and linear network coding to secure the health care information in the cloud. For providing security over stored data and effective exchange of key matrix is achieved through coding and re-encryption. The security of data transfer among the sender and receiver are studied effectively [24]. Omar et al. proposed another patient centric scheme to preserve the data through the block-chain technology to address the concern of decentralization. The pseudonymity of the patient data is ensured through the effective cryptographic functions. The usage of block chain ensured the accountability and security of health care data [25].

Akshay et al. focused a novel Medi-Trust algorithm is proposed by hybridizing the two well-known algorithms of attribute-based encryption and RBAC to secure the privacy of the patient data in the cloud. The data encrypted in the proposed scheme requires two distinct decryption keys to obtain the information. The proposed scheme is evaluated and compared with the existing system [26]. Wang et al. proposed a privacy preserving scheme which is fully homomorphic is proposed to secure the cloud data and prevented the arbitrary behavior of both the doctor and user [27]. Deepa et al. proposed attribute-based file encryption mechanism for preserving the data of patient with effective retrieval mechanism, which is developed with computation of patient key and doctor indexing along with the mechanism of cloud working and decryption of patient report [28].

Wei et al. proposed a novel fine-grained access control approach to secure the health care data against the inference attack and also preserve access policies and role attributes privacy. A blind retrieval data protocol is employed to preserve the data attributes access pattern [29]. Mehmood et al. focused a security scheme is proposed through the elliptic curve cryptography based rotating group signature scheme to preserve the patient anonymity. Additionally, the onion router is established is used to ensure data privacy at the network layer [30].

3 Preliminaries

a) Bilinear Mapping

Bilinear Mapping was employed extensively in the cryptography and signature generation in securing the data in the cloud environment [31]. Let G_a, G_b be an additive group and a Prime Orders multiplicative cyclic group respectively and g be the generator for G_a then the bilinear map that exist between G_a and G_b is given based on the following theories as,

i) Bilinear – $l, \ m \in Z_q^*$, e (gl, gm) = e(g, g)lm = e(gm.gl) for all
ii) Non-degenerate-it will exist only at a point where e (G_a, G_b) $\neq$ 1
iii) Computable-to estimate e (l, m) for any l, m $\in G_a$

The bilinear mapping is used in the setting-up of cloud and signature generation in the proposed framework with novel Threat Aware Revocation algorithm. The group operation over groups G_a and G_b is the basis for generation of hash function.

b) Threat Aware Revocation

The group signature in the proposed framework is generated through the novel Threat Aware Revocation algorithm based on the user attributes. The generated group signature provides the access control over the data in the cloud. The generated signature is updated and modified with secret prime twister algorithm before distributing among the users. The generated signature is stored in the Extended Dynamic Hash Table (EDHT) and used for verifying the user during the cloud access. The signature in the EDHT will be nullified for revoking the user in the cloud.

c) AFT-SBES

The data access control is accomplished through novel Advance Flexi Twister Secret Block Encryption Standard (AFT-SBES) algorithm. The algorithm is based on the Advanced Encryption Standard (AES) cryptography established over the segmented data in the blocks. Similar to the TAR signature, the key generated is updated and modified with secret prime twister algorithm before distributing among the users. The users have to provide the key to decrypt the encrypted data.

4 Proposed Security Model

The novel framework proposed for securing the cloud data through the TAR-AFT framework with two mechanism i.e., access control and data control as in Fig. 1. The TAR-AFT framework involves the owner to upload their encrypted file into the health care cloud. The user decrypts the data through the decryption key. The data is initially split into parts and are stored in the block. The process of both decryption and encryption is performed using the AFT-SBES algorithm over the data that are stored into the block. The entire process of key generation, encryption and decryption of data is utilized for data control mechanism.

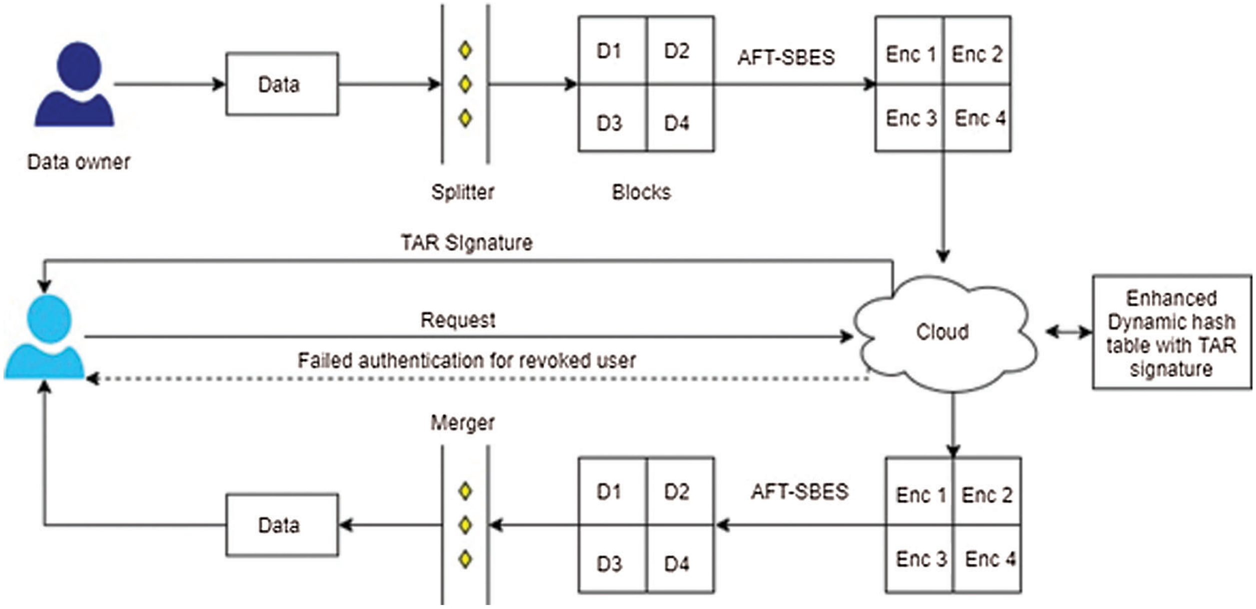

Figure 1: Proposed TAR-AFT Framework

The TAR algorithm is employed for generating the group sig nature and the activities of the user in the clouds are monitored through the SelfSession Shadow technique. The data owner can regulate the addition or removal of new user and existing user in the health care cloud. The data owner has the authority to add or remove the users from the group by providing the group signature or nullifying it in the cloud. the generated user signature is stores in the extended dynamic hash table (EDHT). The generation of signature and its storage along with its verification forms the mechanism of access control over the data. Both the key and signature are used to authenticating the user for their cloud access and retrieving the information without security concern on privacy and confidentiality.

The TAR algorithm is employed for generating the group sig nature and the activities of the user in the clouds are monitored through the Self-Session shadow technique. The data owner can regulate the addition or removal of new user and existing user in the health care cloud. The data owner has the authority to add or remove the users from the group by providing the group signature or nullifying it in the cloud. The generated user signature is stores in the extended dynamic hash table (EDHT). The generation of signature and its storage along with its verification forms the mechanism of access control over the data. Both the key and signature are used to authenticate the user for their cloud access and retrieve the information without security concern on privacy and confidentiality.

For illustration of the proposed TAR-AFT framework, let x be the owner who upload their health data in the form of image in the cloud. Using the image split algorithm, the health record image is split into segments. Each of the segments contains 8 blocks and are encrypted through AFT-SBES algorithm and the encrypted final block is uploaded to the cloud. The key obtained from AFT-SBES algorithm is modified using the secret prime twister algorithm. The modified key is generated for encryption along with the decryption key. When three users i, j, k belongs to different specialization but want to monitor the health status of the owner x. The Cloud Authority (CA) distributes the group signature among the users based on their attributes through which they can access the health care cloud. The modified decryption key is also provided to them to obtain the information of the owner over the encrypted data in the cloud. Similar to the keys the group signature is subjected to updation and modification using random secret prime twister algorithm. The CA performs the verification activity over the digital signature and security keys to allow the access and data decryption. The Self-session shadow tracks the entire activity in the cloud and urge the data owner to carry out revocation of user for their attempt to either violate the privacy policy or perform any unauthenticated activity, the cloud administrator may revoke the signature of the concern person in the EDHT.

The proposed TAR-AFT framework can provide the following security model for securing the cloud data:

Privacy of data: The privacy of the data is ensured through the proposed AFT-SBES algorithm. The file is segmented into parts and encrypted through the 8 blocks with size of 16 bytes. After the termination of encryption process, the last encrypted block alone is uploaded to the cloud. During the decryption process, the user has to download the single block from each segment and decrypt them in reverse order to obtain the information in parts and again the file concatenation process is employed to obtain the original file. Hence, even an attacker or unauthorized user try to access the data, they can obtain only the part of the file which is improper to provide any information. Thus, the privacy of the data is ensured through the proposed TAR-AFT framework.

Confidentiality of data: The confidentiality over the data is ensured through the novel TAR algorithm. The random signature is generated with the user attributes. Every user is provided with the distinct user identity while being assigned to handle the specific record. This mechanism of signature generation through the random secret twister algorithm ensures the confidentiality of data being accessed only by the authorized person. Additionally, the revocation mechanism established with the SSS technique monitors the activities in the cloud. The signature of the user will be nullified for revocation.

5 System Algorithms

The proposed security model involves the following process:

Setup (1^{SP}, N): The cloud is initially established with the receiver set size N with the security parameter SP. The CA executes this algorithm to generate the Public key and Master key which are specified as P_k and M_k. The SP is obtained from the Z_q^* and CA executes the setup algorithm with the bilinear mapping process. Two prime order multiplicative groups G_m and G_{mt} is taken G_{mt} is defined as the squared G_m. The values of a, h, b and β, γ, δ is chosen from G_m and Z_q^* respectively to carry out the process of cryptographic hash function as in equation

$$H_1 : \{0,\ 1\} \to Z_q^*,\ H_2 : \{0,\ 1\}* \to Gm,\ H_3\ Gmt \to Gm\ and\ H_4 :\ Gmt \to Z_q^* \tag{1}$$

Finally, it yields the system public key $P_k = (h, h, h^{\gamma}, h^{\beta^N}, h^{\delta} \ldots)$ and the master key $M_k = (a, b, \beta, \gamma, \delta)$.

Output: The Public Key P_k and Mater Key M_k is generated.

Add Data owner (OD): The owner is enrolled into the cloud through their attributes and the CA executes this algorithm to generate the owner identity O_{ID} through which they communicate in the cloud.

Input: Attributes of the Data Owner

When the owner requests the cloud to add them, their attributes are obtained and processed with the generated O_{ID} using the Eq. (2)

$$O_i = a^{(\beta + H_1(OID_i\ ))\prod_{j=1}^{n}(\beta + H_1(OID_j))} \tag{2}$$

Output: The owner is added to the cloud with new owner identity O_{ID}.

KeyGen (M_k, O_{ID}, A_P): The Identity of Data Owner O_{ID} is used along with the Master Key M_k and Access Policy A_P of the cloud and the key is generated. The ASCII value for each character in generated key is added to the random prime number in the secret prime twister algorithm and it is modified with either forward or reverse process block.

Add User (U_A, O_{ID}): Based on the data owner attributes details, the CA adds the user through their attributes (U_A) along with the data owner identity (O_{ID}). The registered users are added to the cloud through this algorithm with their identity U_{ID}.

Input: U_N, U_A, O_{ID}

The CA on obtaining the user details and generates the identity U_{ID} and they are added to the health care cloud. using the equation

$$U_i = a^{(\beta + H_1(UID_i\ ))\prod_{j=1}^{n}(\beta + H_1(UID_j\ ))} \tag{3}$$

Output: User is added in the cloud

Sign-gen (A_P, U_{ID}, M_k): On adding the user, the CA runs this algorithm to randomly generate the digital signature (UD) for the concerned user using their identity and master key. The access policy is also included to provide effective access control.

The U_{ID} contains the information of user and it is integrated with the health care cloud master key to generate the random signature. Upon the generation, it follows the same procedure as in keygen to update the signature with random prime number and modify it in the secret twister.

Output: digital signature (D_s) for user

Segment (data): The owner data in the proposed framework is partitioned into segments for encryption to achieve the data privacy and confidentiality.

Enc (M, U_{ID}, A_p, b_j): The data is encrypted over the eight sequential block for each segment of splitted file. The encryption key of bit size 128 is used to encrypt the data in the sequential blocks (b_j) of size 4 × 4. The uploading file of data owner is encrypted with the message M based on the U_{ID} and $A_{p.}$

Integrate (PI_i): The partitioned file is reconstructed to obtain a single file in the proposed framework.

Revoke (U_{ID}, U_A): The CA monitors the activity of the cloud through the Self-session shadowing and when any user involves in any unauthorized activities, they are revoked from the cloud through the nullification of their signature U_A.

Input: U_{ID}, U_A

The process of revocation is carried out through the following equation

$$R_i = a^{\prod_{j=1,\, j\neq k}^{n}(\beta + H_1(UID_j\,))} \tag{4}$$

Output: revocation of user from the group.

Algorithm 1: Secret Prime Twister

```
Secrettwist(key K)
        K1 is set of interchanging byte values of K (swapping)
        K2 is set of interchanging byte values of K (swapping)
        K1 = {Set of Key Bytes}
        K2 = {Set of Key Bytes}
Random selection (K1,K2)
If selection (K1)
Begin
        K1 as input
        K1 = twistblock (K1)
End;
Else
Begin
        K2 as input
        K2 = twistblock (K2)
End;
twistblock(Block B)
for each $B_{i,\ i \in 1 \text{ to } n}$
     Ai = A Value of $B_i$
$RP_i$ = RP value of $B_i$
     $B_i$ = Ai ⊕ $RP_i$
end for
return Block
```

Algorithm 2: Digital Signature Generation

```
Input: $U_{ID}$, $M_k$, $A_p$
begin
for each $U/O_{i,\ i\ \in\ 1\ \text{to}\ n}$
get the security parameters from cloud setup
get the User/Owner identity and attributes
generate the digital signature DS
    Ds= twistblock(Ds)
    Updated Ds stored in EDHT
end for
end
```

Algorithm 3: Data Encryption

```
Input : File, $A_p$, $K_s$, $O_{ID}$
Get the key
Partition the key into n blocks
$K = \{K_1, K2 \ldots K_n\}$
For each $K_{i,\ i\ \in\ 1\ \text{to}\ n}$
    Begin
        Invoke Secrettwist($K_i$)
UPDATE($K_i$)
    End;
End for;
Get the file to be encrypt from the data owner
//Partition the file S into Segments
$S = \{FS_1, FS_2 \ldots FS_n\}$
//Partition each segments into blocks
for each $FSi_{i\ \in\ 1\ \text{to}\ n}$
$B = \{b1, b2 \ldots bn\}$
for each $B_{i,\ i\ \in\ 1\ \text{to}\ n}$
begin
for each UPDATED $K_{j,\ j\ \in\ 1\ \text{to}\ n}$
$C_j = B_i \oplus K_j \oplus C_{j-1}$
endfor
$CF_i = C_{j-1}$
end for
Upload $CF_i$ Ciphertext in cloud.
end for
```

Algorithm 4: Data Decryption

```
Input : File, $A_p$, $K_s$, $U_{ID}$
User send request to Cloud access file
//get the decryption keys
get the key set K = {$K_1$, K2 … $K_n$}
get the encrypted segments
S = {$FS_1$, $FS_2$ … $FS_n$}
for each $FSi_{i \in n \text{ to } 1}$
B= {b1, b2 … bn}
for each $B_{i,\ i \in n \text{ to } 1}$
begin
for each $K_{j,\ j \in n \text{ to } 1}$
$M_j = B_i \oplus K_j \oplus C_{j-1}$
endfor
$M_i = C_{j-1}$
end for
download $M_i$ plaintext.
end for
```

6 Simulation Result

The TAR-AFT framework for securing data in cloud data is established in Java and it employed the drop box for storage. The web services are hosted in Apache Tomcat and JAX-WS as web service that forms the interfaces in the cloud. The clouds custom MYSQL database is simply interchanged with other databases at data storage in server-side. The Java supported browser formed the client-side. The secure implementation on storage and retrieval of data is carried through Amazon web service. The other configuration involves i7 processor, 16 GB RAM, along with 1TB hard disk.

Signature Generation

The proposed TAR algorithm generates the group signature in the TAR-AFTframework to provide effective access control. The efficiency of the signature generated is (s.pair)+Mul+ Exp, in which the total of data item number is represented as s, both Mul and Exp represent the multiplication and exponential of G and pair is the pairing computation. The time involved in signature generation and proofing through the TAR algorithm is given in Fig. 2. The time and efficiency for generating and proofing the group signature largely depend on the number of users involved as a group to handle the health care data of owner.

The user communication cost for TAR-AFT framework is found to be 950 kb whereas the existing AES and AES-CP-IDABE has the cost of 1000 kb. The execution time for each user in the TAR-AFT framework is about 160 ms and it is lower than the time consumed by both the AES and AES-CP-IDABE frameworks as in Fig. 3.

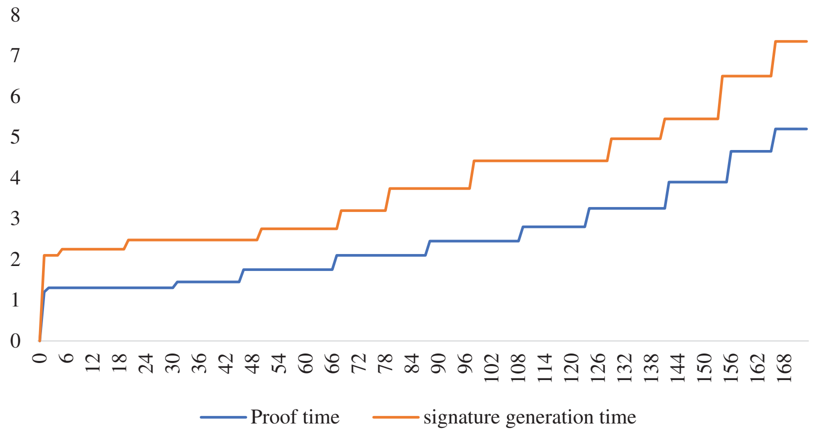

Figure 2: Time for signature generation and proof time for TAR-AFT

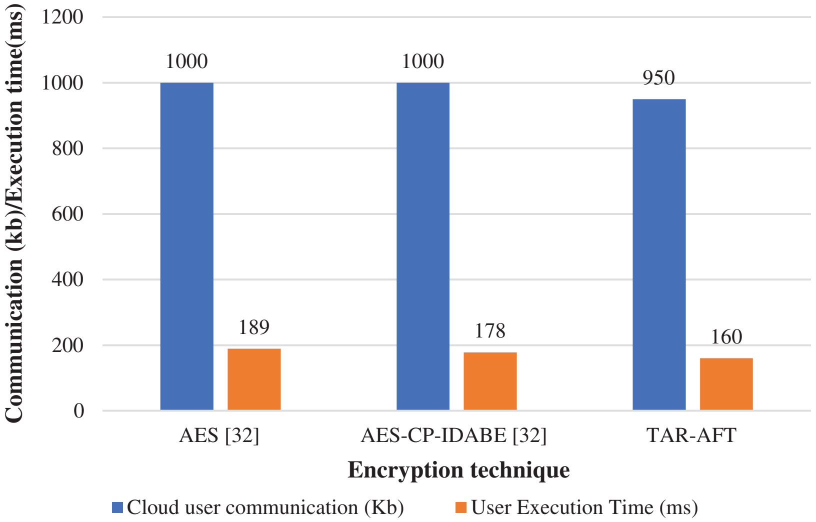

Figure 3: Performance on execution time and communication cost of user

The performance of the proposed TAR-AFT over the communication cost of data owner is given in Fig. 4. Similar to the existing framework, the cost increases with increase in number of users. The cost involved for 500 users in the cloud is about 820 kb which is less than the 895 kb and 990 kb for AES-CP-IDABE [32] and AES respectively.

The encryption time for different data size over the different attributes is given in Fig. 5. The time involved for encryption through the proposed TAR-AFT is more than the existing model when the number of user attribute is less. However, with the increase in number of attributes, the time involved for encryption decreases than the existing framework and the similar pattern is observed over the decryption time for various data size. The comparison over the existing framework of I-CP-ABE [31] and AES-CP-IDABE [32] is given in Fig. 6.

The proposed TAR-AFT Framework is compared with the other existing models in Tab. 1. The comparison is specified over several security requirements. The proposed TAR-AFTsupport multiple authentications for handling several users in the health care cloud and it is completely based on cloud environment. It can provide the fine-grained access control through the novel group signature and preserve the privacy of health data of owner. The proposed system provides effective scalability through the block data encryption. With effective monitoring and user revocation mechanism the confidentiality of the data is ensured and the cloud is resistant against the collusion attack.

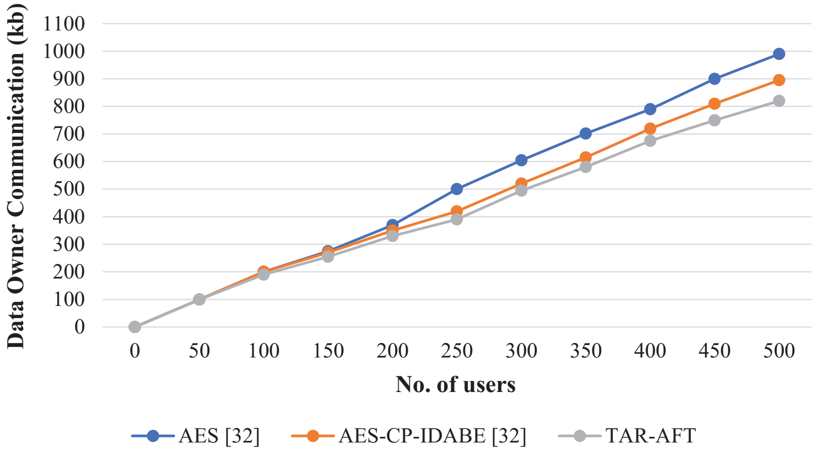

Figure. 4: Performance on data owner communication

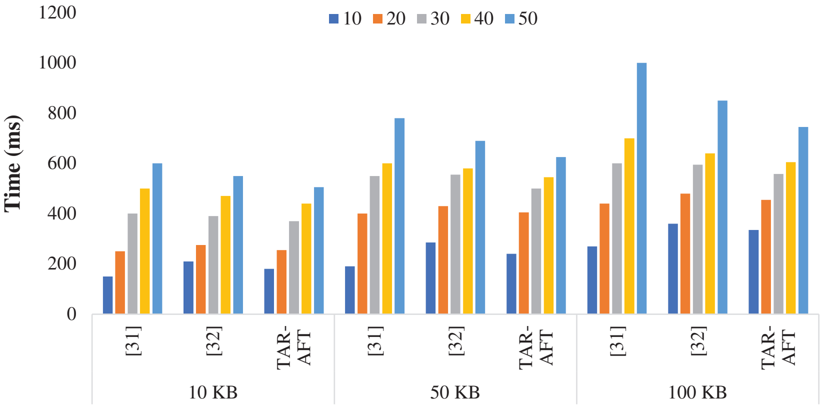

Figure 5: Data size *vs.* encryption time over different number of attributes

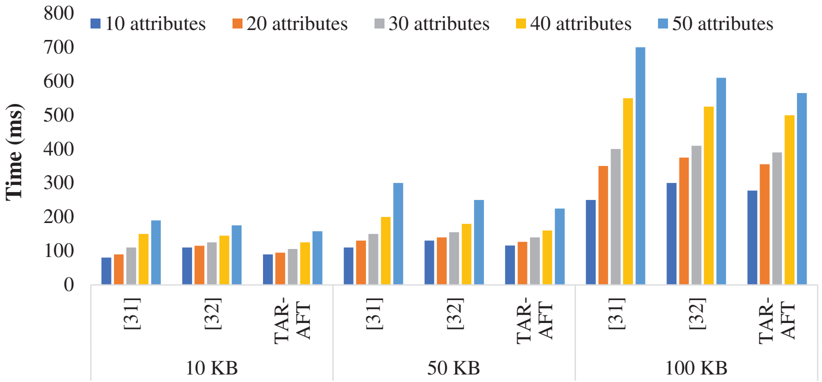

Figure 6: Data size *vs.* decryption time over different number of attributes

Table 1: Comparison with the existing models

Security requirement	MA-ABE [33]	EHRPC-ABE [34]	KP-ABE [35]	HMA-CP-ABE [20]	TAR-AFT
Multiple authentication	No	No	No	Yes	Yes
Cloud based	Yes	Yes	Yes	Yes	Yes
Fine grained access control	No	Yes	Yes	Yes	Yes
Data privacy	Yes	Yes	Yes	Yes	Yes
Efficiency	Medium	High	Average	High	Very high
Scalability	No	Yes	No	Yes	Yes
Data confidentiality	Yes	Yes	Yes	Yes	Yes
Collusion resistant	Yes	Yes	Yes	Yes	Yes
Multi/single stage AA	Multi	Single	Single	Multi	Multi

7 Conclusion

A novel framework of TAR-AFT is proposed for ensuring and preserving the privacy and confidentiality of the owner data in the health care cloud. For the proposed framework, the owner data is considered to be in image form. The owner and the user who are involved in the cloud are provided with distinct identities to protect their privacy. The proposed framework involved two novel algorithms in the form of TAR and AFT-SBES for group signature generation and key generation respectively. Both the signature and the key are updated and modified through the ASCII values and secret twisting mechanism. The user is provided with the group signature and key to access the cloud and data. The activities of the cloud are monitored through the SSS approach and it supports the revocation of user under any suspicious activities. Hence both the confidentiality and privacy of the owner data is achieved. The proposed framework is evaluated for its performance on encryption and uploading time, downloading and decryption time. All the time measures increase with respect to the operating file size. The signature generation and verification time increases with the increasing number of users and is very robust with high efficiency. The proposed framework is compared with the other security model in the health care cloud and validated its effectiveness in it. The future work may involve some diagnostic approaches to handle vast amount of owner data without compromising on privacy and confidentiality. Similarly, the proposed framework can be implemented over the text data to determine its practicality in real-time scenarios.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," *Journal of Network and Computer Applications,* vol. 79*,* pp. 88–115, 2017.

[2] B. K. Sarkar, "Big data for secure healthcare system: A conceptual design," *Complex and Intelligent Systems,* vol. 3*,* no. 2*,* pp. 133–151, 2017.

[3] J. D. Ferrer, O. Farras, J. R. Gonzalez and D. Sanchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," *Computer Communications,* vol. 140*,* pp. 38–60, 2019.

[4] H. O. Alanazi, A. A. Zaidan, B. B. Zaidan, M. M. Kiah and S. H. Al-Bakri, "Meeting the security requirements of electronic medical records in the ERA of high-speed computing," *Journal of Medical Systems,* vol. 39, no. 1, pp. 165178, 2015.

[5] D. F. Sittig and H. Singh, "A new socio-technical model for studying health information technology in complex adaptive healthcare systems," *Cognitive Informatics for Biomedicine,* vol. 14, no. 2, pp. 59–80, 2015.

[6] M. Cifuentes, M. Davis, D. Fernald, D. R. Gunn, P. Dickinson *et al.,* "Electronic health record challenges, workarounds, and solutions observed in practices integrating behavioral health and primary care," *The Journal of the American Board of Family Medicine,* vol. 28, no. 1, pp. 63–72, 2015.

[7] R. Miotto, L. Li, B. A. Kidd and J. T. Dudley, "Deep patient: An unsupervised representation to predict the future of patients from the electronic health records," *Scientific Reports,* vol. 6, no. 6, pp. 1–10, 2016.

[8] Y. Miao, X. Liu, K. K. R. Choo, R. H. Deng, J. Li *et al.*, "Privacy-preserving attribute-based keyword search in shared multi-owner setting," *IEEE Transactions on Dependable and Secure Computing,* vol. 18, no. 3, pp. 1080–1094, 2021.

[9] M. A. Sahi, H. Abbas, K. Saleem, X. Yang, A. Derhab *et al.,* "Privacy preservation in e-healthcare environments: State of the art and future directions," *IEEE Access,* vol. 6, pp. 464–478, 2017.

[10] R. Parks, H. Xu, C. H. Chu and P. B. Lowry, "Examining the intended and unintended consequences of organisational privacy safeguards," *European Journal of Information Systems,* vol. 26, no. 1, pp. 37–65, 2017.

[11] Z. Wang, "Provably secure key-aggregate cryptosystems with auxiliary inputs for data sharing on the cloud," *Future Generation Computer Systems,* vol. 93, pp. 770–776, 2019.

[12] X. Mao, X. Li, X. Wu, C. Wang and J. Lai, "Anonymous attribute-based conditional proxy re-encryption," *Lecture Notes in Computer Science,* vol. 12, pp. 95–110, 2018.

[13] R. R. Al-Dahhan, Q. Shi, G. M. Lee and K. Kifayat, "Survey on revocation in ciphertext-policy attribute-based encryption," *Sensors,* vol. 19, no. 7, pp. 1695–1710, 2019.

[14] L. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal,* vol.22, no. 2, pp. 172–183, 2020.

[15] P. B. Prince and S. J. Lovesum, "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system," *SN Computer Science,* vol. 1, no. 5, pp. 1–8, 2020.

[16] J. Liu, H. Tang, R. Sun, X. Du and M. Guizani, "Lightweight and privacy-preserving medical services access for healthcare cloud," *IEEE Access,* vol. 7, pp. 106951–106961, 2019.

[17] A. S. Babrahem and M. M. Monowar, "Preserving confidentiality and privacy of the patient's EHR using the OrBAC and AES in cloud environment," *International Journal of Computers and Applications,* vol. 12, pp. 1–12, 2018.

[18] A. Omar, M. Z. Bhuiyan, A. Basu, S. Kiyomoto and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on block chain environment," *Future Generation Computer Systems,* vol. 95, pp. 511–521, 2019.

[19] X. Chang, N. Wang, L. Zhu, K. Sharif and C. Zhang, "Achieving searchable and privacy-preserving data sharing for cloud-assisted E-healthcare system," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8345–8356, 2019.

[20] S. Sharaf and N. F. Shilbayeh, "A secure G-cloud-based framework for government healthcare services," *IEEE Access,* vol. 7, pp. 37876–37882, 2017.

[21] M. K. Kundalwal, K. Chatterjee and A. Singh, "An improved privacy preservation technique in health-cloud," *ICT Express,* vol. 5, no. 3, pp. 167–172, 2019.

[22] A. Mubarakali, M. Ashwin, M. Dinesh and A. Dinesh Kumar, "Design an attribute based health record protection algorithm for healthcare services in cloud environment," *Multimedia Tools and Applications,* vol. 79, no. 5, pp. 3943–3956, 2020.

[23] K. A. Shakil, F. J. Zareen, M. Alam and S. Jabin, "BAMHealthcloud: A biometric authentication and data management system for healthcare data in cloud," *Journal of King Saud University-Computer and Information Sciences,* vol. 32, no. 1, pp. 57–64, 2020.

[24] K. J. Modi and N. Kapadia, “Securing healthcare information over cloud using hybrid approach,” *Progress in Advanced Computing and Intelligent Engineering,* vol. 12, no. 23, pp. 63–74, 2019.

[25] A. Omar, M. S. Rahman, A. Basu and S. Kiyomoto, “Medibchain: A blockchain based privacy preserving platform for healthcare data,” in *Int. Conf. on Security, Privacy and Anonymity in Computation, Communication and Storage*, Nanjing, vol. 2, pp. 534–543, 2017.

[26] A. Tembhare, S. S. Chakkaravarthy, D. Sangeetha, V. Vaidehi and M. V. Rathnam, “Role-based policy to maintain privacy of patient health records in cloud,” *The Journal of Supercomputing,* vol. 75, no. 9, pp. 5866–5881, 2019.

[27] X. Wang, L. Bai, Q. Yang, L. Wang and F. Jiang, “A dual privacy-preservation scheme for cloud-based eHealth systems,” *Journal of Information Security and Applications,* vol. 47, pp. 132–138, 2019.

[28] N. Deepa and P. E. Pandiaraja,“Health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption,” *Journal of Ambient Intelligence and Humanized Computing,* vol. 1, no. 1, pp. 1–11, 2020.

[29] C. Mathuvanesan and T. Jayasankar, “Performance analysis of singularity and irregular detection in human health monitoring using lipchitz exponent function,” *International Journal of Engineering Research and Technology,* vol. 2, no. 6, pp. 414–418, 2013.

[30] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston and Y. Zhang,“Anonymous authentication scheme for smart cloud based healthcare applications,” *IEEE Access,* vol. 6, pp. 33552–33567, 2018.

[31] X. Shumin and C. Ren,“Security protection of system sharing data with improved cp-abe encryption algorithm under cloud computing environment,” *Automation Control Computing, Science,* vol. 53, pp. 342–350, 2019.

[32] S. Chandel, G. Yang and S. Chakravarty,“AES–CP–IDABE: A privacy protection framework against a dos attack in the cloud environment with the access control mechanism,” *Information,* vol. 11, no.8, pp. 372–381, 2020.

[33] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” IEEE *Transactions on Parallel and Distributed Systems,* vol. 24, no. 1, pp. 131–143, 2012.

[34] R. Arunprakash, T. Jayasankar and K. VinothKumar, “Biometric encoding and biometric authentication (beba) protocol for secure cloud in m-commerce environment,” *Application of Mathematical Information Science,* vol. 12, no. 1, pp. 255–263, 2018.

[35] Q. Li, H. Xiong, F. Zhang and S. Zeng, “An expressive decentralizing kp-abe scheme with constant-size ciphertext,” *International Journal of Network Security,* vol. 15, no. 3, pp. 161–170, 2013.