Mobile Networks and Applications (2019) 24:1755–1762
https://doi.org/10.1007/s11036-019-01379-4

An Attempt to Design Improved and Fool Proof Safe Distribution of Personal Healthcare Records for Cloud Computing

P. Preethi[1] · R. Asokan[1]

Published online: 26 October 2019

Abstract
In the recent gears applications such as personal health care are broadly made use by the diseased individuals for preserving and organizing their medical information over a private, secure and trustful computing. They make use of the service providers as third party environment for interchanging the medical records of the diseased individuals. The cloud computing permits effective management and circulation of private and personal medical related records which always faces challenges in terms of various safety associated characteristics like discovery and existence of vulnerable medical data by the illegal users. To provide safety and confidentiality it is mandatory to accomplish the data before contracting out and only the authorised users are allowed to make use of the data. Hiding the information of the users are important during gaining access to the data present over the network. Moreover for reducing the setbacks in safeguarding the key of the data containers the personal health records are classified into several associated fields. For wrapping the information of the user's unsigned verification based on the element based encoding (EBE) is employed and fine grained data access control based on the advanced encryption scheme are tailored. The comprehension provides an advanced level of security and confidentiality for the personal health records. The scheme permits autonomous alterations of the admission policies or file entities along with the autonomous user cessation. Additional analyses and evaluations reveals that the designed scheme is effective in terms of safety and secrecy.

Keywords Personal health records · Cloud computing · Element based encoding · Advanced encryption standard and confidentiality

1 Introduction

The cloud technologies are rapid booming technique comprising all the IT related wealth offered as services with the aid of the internet. The significant service provision models like software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) adorning cloud serving as the overall constitution of the service-oriented framework [1]. The cloud-related services are implemented broadly because of its cheap availability and expandable service dissemination platforms.

Over the present day, the personal health records are designed as the budding development in health-related technologies. The cloud platform permits the patient to generate, organize and manage their personal health-related information irrespective of place with the aid of internet aiding storage, recovery and distribution of health-oriented data more effectively. Mainly every patient is assured for comprehensive authority over their medical related records. It is possible for a patient to distribute their information over a broad variety of users comprising the suppliers of healthcare or associated members based on their necessity and motivation. It is thrilling to hold an opportune personal healthcare record services for every person where diverse safety and confidentiality related threats prevail within the cloud computing environment. Because of the increased expense of generating and preserving dedicated information centersseveral health record related services are contracted out or offered by the third party suppliers, for instance, Google Drive, iCloud and Dropbox [2]. Normally the cryptography based encoding and decoding schemes are employed for safety [3].

The RSA schemes could be employed for encoding the information before it is contracted out within the cloud environment. Therefore for recuperating the information, the user

✉ R. Asokan
principalkncet@gmail.com

P. Preethi
preethi1.infotech@gmail.com

[1] Kongunadu College of Engineering and Technology, Trichy, Tamil Nadu, India

may demand the key manager for creating the public key offered that the user is verified individual [4]. Earlier analyses on safety disclose that for assuring safety over cloud there prevail three safety-related techniques as hash creation scheme, captcha scheme and AES scheme that are broadly employed [5]. Presently the digital signature is employed for verifying and AES encoding scheme offers information privacy [6].

The ultimate ideology is regarding the patients having the ability to manage the distribution of their vulnerable and personal health-related data mainly during their storage over the third party server that is not fully basedon the individuals. The personal health record system has the capability to restrict the access management of the users to aid the application. For accomplishing the access strategies are linked with several sets of user elements. For enhancing the ideology the information is encoded based on a set of objects due to which various users cannot keep accurate keys for accessing the needful data [7]. It might generate efficient encoding along with key safeguarding allowing a secure multi – generator mechanism which is mandatory for the multi – access network where the data can be distributed in a secure manner over the undependable cloud environment [8].

The feature-based encoding (FBE) comprises exclusive characteristics of averting the user agreement to a crucial extent for accomplishing fine-grained management a ciphertextfeature-based encoding (CT – FBE) is employed [9]. The feature-based encoding (FBE) is a public key based encoding where a secret key of a user and ciphertext are reliant over the elements [10]. Normally the explorations over the encoded documents are quite intricate and time exhaustive where the machine coded.

There prevails few modeling for safeguarding the cloud associated information for which diverse analyses are performed for improving the safety over cloud encoding. The rest of the paper is organized as the discussion of cloud safety is detailed in section 1. Section 2 delivers the prevailing schemes designed by diverse scholars for designing a better system. Section 3 provides an overview of the prevailing schemes and depicts the ideology of the designed scheme along with the algorithms, section 4 affords the performance analysis in terms of different file sizes and section 5 provides overall conclusion of the designed scheme.

2 Related work

Diverse safety related mechanisms are prevailing presently for distributing data over the untrusted servers. The schemes permit the creator of the information to store the encoded files over these untruthful storages and broadcasting the related keys for decoding uniquely to the verified users. Therefore it is supposed that the unverified users could not discover the data files hoarded onto the server. Here for fulfilling the purposes advanced encryption scheme serves as the key encoding primeval.

The design of an encoding scheme employs the swapping and permutation techniques where the initial intention is to organize the information based on the elements permitting access governance and AES for safeguarding the patient's records [10]. The assessment of cloud safety related schemes is carried out based on the linear mechanisms based on varied performance metrics. The outcomes of simulation reveal that advanced encryption standard works quicker and serves as a safer scheme [12]. The advanced encryption standard is employed broadly in various platforms and verified against diverse safety-related applications.

The attempt was to restore the access permissions of the user by employing two schemes such as element based encoding (EBE) and proxy re-encoding over peer to peer cloud storage which makes the information safe over the cloud. The prevailing schemes are costly in terms of time and effectiveness as evaluated against the advanced encryption standard [13]. The modeling of a scheme termed as a secure hash scheme for efficient verification allows encoding the file employing advanced encryption standard for assuring scattered liability. The sender performs hash over the file and forwards to the target recipient where the hash is carried out once again followed by which hash match is verified [14]. The secure hash scheme aids in creating an extended hash value which is more conflict tolerant which is employed in a broader perspective.

The assessment of the performance of the encoded repository is carried out for encoding immense repository employing non – a linear key scheme which is minimal as estimated against the linear key schemes. Therefore the non – linear key scheme could be employed [15, 16] for encoding minimal key values. Usually, the log-based files catalogs the access related information of each and every user of the information. It is because the log files are not encoded the confidentiality is not sealed. Since it discloses the user unsigned information there are no safety assurances for health records which paves way for incorrect verification and information safety. Primarily the secure hash scheme is employed for verification since it safeguards the reliability of the information and semantic values of elements after performing hash operations. Even though the scheme is employed in a broader perspective it offers only one-way hash which makes it impossible to aid encoding and decoding of information over the storage. Furthermore, the scheme is not up to the level in performing computation and holds well-known safety threats.

3 Formulating problem

For several systems such as the preservation of health records, a supervising authority (SA) agrees to accomplish key

preservation for the proficient users. Still, it needs increased belief for unique authority which may run short for a key for the encoded information [11]. But there still remain a benefit of making use of fresh encoding model termed as element based encoding (EBE) where the scheme serves as user elements or the information choose the access strategies allowing the patient to carefully distribute the personal health records among the collection of users by encoding the file over a collection of elements without the necessity to learn comprehensive catalog of users [12]. Based on which element count comprised decides the difficulties in encoding, the creation of keys and decoding. The multi-authority element based encoding scheme is employed for offering several authority based access governance schemes.

Several scholars have performed assessments for diverse schemes and aggregation of diverse schemes for safeguarding the information over the cloud environment where an appropriate aggregation of schemes for verification and permission might aid in effective expandable and safer information storage [15].

The health records are preserved over the scattered cloud environment for guaranteeing the patient's governance access over their own personal health records where the talented scheme is encoding the personal health records before subcontracting [13]. In order to guarantee the safety of the information,the advanced encryption standard scheme is employed.

There may be possible chances for imposters to stench the signature of the verified user's vulnerable information stored in a remote server might be misleading. For diverse systems, an inherent postulation is essential where every user holds some individual and located data linked with them which are made use by them to establish their identity [14]. Several verification standards are effortless where the transmission could be simply captured and the information could be often be made use autonomously without the consciousness of the creator. In order to avert the vulnerable user's unsigned verification could be optimistic based on the positive cryptographic model [16]. For accomplishing the needs the element based encoding (EBE) scheme is raised for encoding user verification-related information. In-depth analysis of element based encryption is not used for verification but the outcome of assessment verifies that the element based encryption (EBE) aids an effective unsigned verification.

Based on the element based encryption (EBE) the access strategies are portrayed based on their elements of the user information permitting a patient to choose and distribute their personal health record among the set of users by encoding the file over a collection of elements without the requirement of learning a comprehensive list of the users. The encoding and decoding process is performed based on advanced encryption standard which is the primarily used encryption. The encoding is performed over a precise count of iterations allowing the information to be safer.

3.1 Model description

The intention is to offer a detailed information of the framework of the user unsigned verification system as portrayed in Fig. 1 comprising three elements.

3.1.1 Cloud service supplier

It offers information storage and restoring services for the promising users where the creator of the information stores them in an encoded format where only the privileged users could restore the encoded information from the storage and then it is decoded over the user side by acquiring the suitable key for decoding from the creator of the information. It is considered that the service suppliers of the cloud aresemi-trusted based on the standards prevailing within the system. Moreover, it is regarded that it attempts to gain knowledge about the data over the encoded contents during querying and acknowledgment process as possible with vulnerable intention. For the designed scheme the key for decoding is straightforwardly sent to the user where the service suppliers could not hinder in communicating the decoding key to the user.

3.1.2 Belief authority

The user verification is carried out by accepting suitable elements and verification key where the key is created by the belief authority prevailing within the server. It generates a public parameter along with the secure master key where the preliminary key concepts for the overall process of the modelled scheme. Moreover it generates user accurate and private keys corresponding to these set of objects for acquiring access to the data, decoding of cipher text and unsigned key for the receivers.

3.1.3 Creator of the information

It is the cloud storage subscription requiring uploading their information over the cloud after decoding. The encoded data could be distributed with the needed receivers with suitable recommendations. The patients could gain access to the records as and when demanded. The verification principles accomplished to gain access to the health record are purely based on the provided permission. For multiple information conditions, it is designed to preserve the health record in a responsive way. The key preservation concept is designed to accomplish the encoding of elements. Here the difficulties are improved among the creators and the users. The access permission is deprived of from various users based on the medical records for several intentions. Figure 2 portrays the process of encoding information storage and restoring.

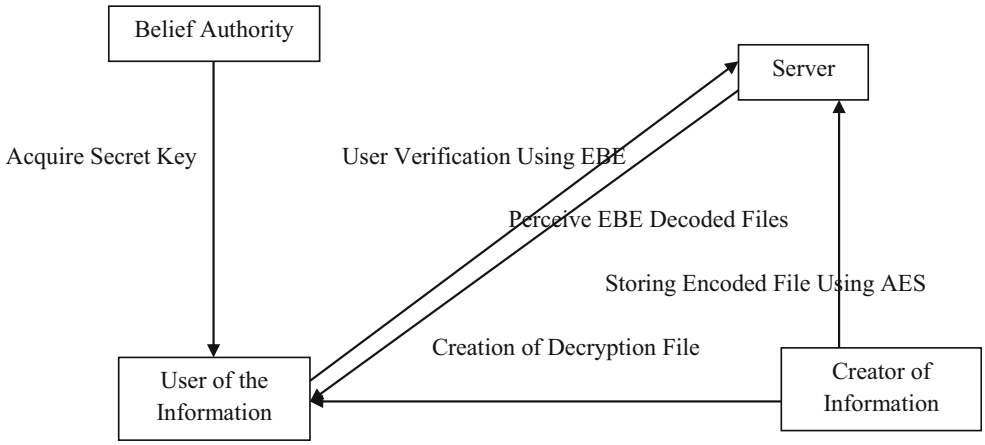

Fig. 1 Framework for Unsigned User Verification

3.2 Designed scheme

The key motivation of the model is to offer safe patient-focused access to their personal health records and efficient key maintaining. The preliminary intention is to divide the system into various privacy related domains such as public and private in terms of the various user linked data access requirements. The personal medical record comprises users having the ability to make access to their professional roles like doctors, nurses and medical scholars. Commonly the health can possibly be

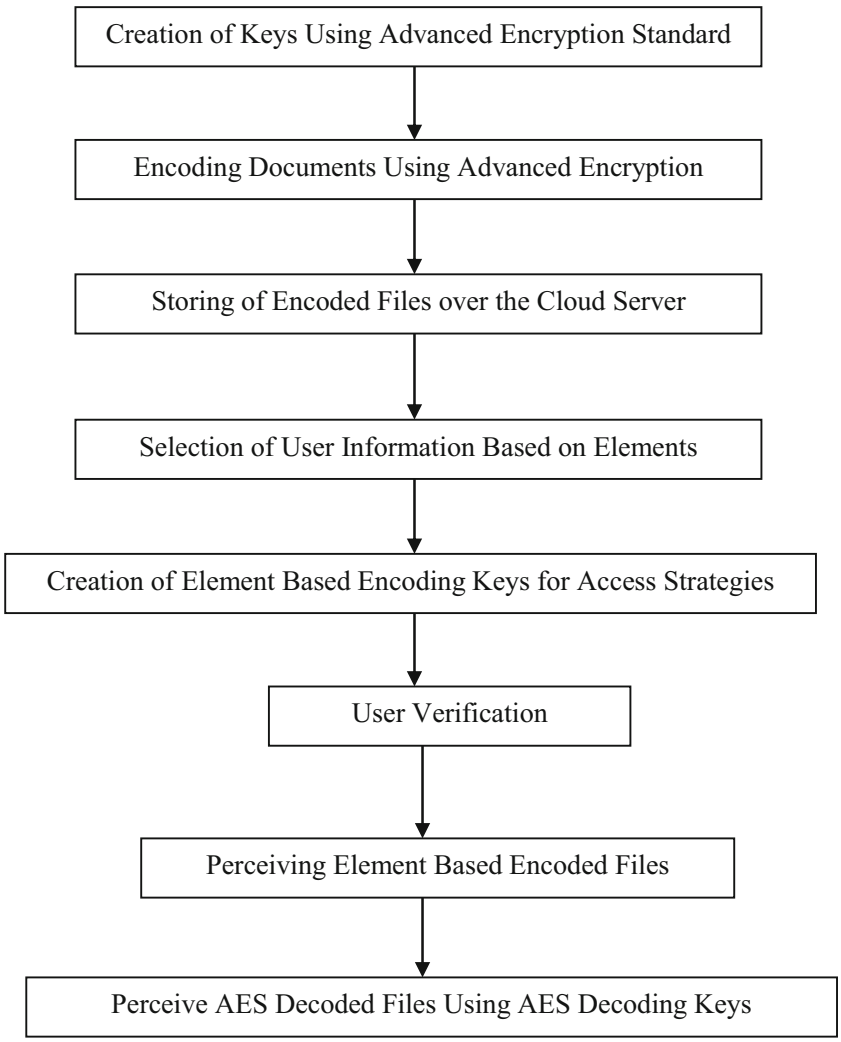

Fig. 2 Flow Diagram of Encoded Information Storage and Revival

matched to a self – determining domain within the society like healthcare, government or insurance fields. Several users can possibly gain access to the personal health records based on their privileges allocated by the creator.

Based on the prevailing assessments based on a secure hash scheme for verification it does not do any justice in delivering enhanced safety. For gaining access to the personal health records approval to health records assures an increased level of safety. Soon after storing the health records into the server the possessor repossesses the key from their mail to gain access to the actual information. The information is encoded and stored into the cloud server. Every possessor of the information like patients is the only belief authority making use of element based encoding for preserving the secret keys and access privileges of the users. For fulfilling the access to the personal domain every personal health record is tagged based on their information elements with linear keys along with file classes which a user could gain access. Based on the user count within personal domain they are usually minimal which reduces the trouble for the possessor. The possessor of the information requires to learn the features of the internal information related to the personal domain for encoding the information. With the aid of user privileges access to the health records are motivated while the vulnerable information is wrapped with the aid of element based encoding scheme.

The possessor stores the element based encoded personal health records into the server. Every possessor files are encoded based on the element based encoding system over a precisely fine-grainedand responsibility based access using a chosen set of information elements permitting the user access to the personal domain. Here the access framework is connected with the key and the objects are connected with the encoded text allowing the authorized users to perform choices over the encoded text. Hence the key policy object based encryption is tailored toa personal domain. It offers safety for the vulnerable data hoarded distributed onto the cloud which thereby minimizes the overheads in assessments of the cloud servers. It is possible only for verified users to decide the personal health record files.

The system aids critical access under extreme conditions. The medical team could gain access momentarily during critical conditions of the patients. Moreover, the medical team demands and acquires the secret key from the critical department which has to be verified by the medical team demanding for the key.

3.3 Element based encoding (EBE) scheme

The element-based encoding (EBE) is a reasonably current mechanism which reassesses the ideology of the public key cryptosystem. In terms of the conventional public key cryptosystem the message is possibly encrypted for an exact users based on the public key of the receiver. The characteristics based cryptography and precisely the characteristics based encoding altered the conventional perceptive of the public key cryptosystems by allowing the public key to be an object string for instance email of the receiver. The element-based encoding stands one level advanced and portrays the characteristics not minimal as a collection of elements such as responsibilities and messages could also be encoded in terms of subsets of elements or strategies portrayed over a collection of elements. The scheme is split into four components comprising the creation of keys.

3.3.1 Initiation (i_p, g) → (p_m, s_k)

The initiation is performed based on the safety metric 'i_p' as input and a global portrayal 'g' portraying a set of permissible elements within the system. It produces the public parameters such as public key 'k_p' and master secret key 'k_m'.

Initialization phase
Input: $x \in e_1$ and $y \in e_2$ from a set of element E
Result: Public key k_p (e_1, e_2, x, y, x_δ, α q), f $\{e_1,\ldots\ldots,e_n\}$, master private key k_m (x_δ)
Select arbitrary φ and $\delta \in a_r$
$x_\delta \leftarrow [\delta]x$
$x_\varphi \leftarrow [\varphi]x$
$\alpha \leftarrow f_{opt}(y,x)^{\varphi}$
for i ← 1 to E do
create the point $E_i \in e_1$
end for
$k_p \leftarrow (e_1, e_2, x, y, x_\delta, \alpha q)$, f $\{e_1,\ldots\ldots,e_n\}$
$k_m \leftarrow (x_\varphi)$
return k_p, k_m

3.3.2 Encoding (p_k, m, s_e) → c_t

The encoding scheme considers the public parameters 'k_p', message 'm' and set of elements 's_e' as input and generates a ciphertext 'c_t' associated with the set of elements.

Encoding phase
Input: Message m, k_p, access model 'f'offered as g x t matrix and $i_p \subset \{1, 2,,\ldots..,g\}$ as $i_p = \{p(i_p) \in E\}$
Result: Cipher text 'c_t' = $\{f, t, c_t, (c_1, d_1),\ldots..,(c_g, d_g)\}$
Create arbitrary vector $a_u = (m, q_1,\ldots..,q_n) \in a_r$
Estimate the column vector $\Omega = ma_u$
Create additional arbitrary vector $p = (p_1,\ldots..,p_n) \in a_r$
$c = m \oplus E (\alpha^m)$
$c_t = [m]q$
for i = 1 to a_u do
$c_i \leftarrow [\Omega_i]\, x_\delta - [p_i]\, E$
$d_i \leftarrow [p_i]q$
end for
$c_t = \{f, t, c_t, (c_1, d_1),\ldots..,(c_g, d_g)\}$
return c_t

Table 1 Analyzing Time Needed by Different Encoding Schemes

File Size in KB	DES	RC4	AES	EBE
1000	1.80	3.98	1.90	4.5
2000	5.90	5.0	5.2	5.5
3000	8.0	7.25	7.5	8.75
4000	9.2	9.1	9.25	9.99
5000	12.99	12.2	13	13.5

3.3.3 Creation of keys (m_k, f) → s_k

The generation of keys produces a secret key 'k_s' by taking master secret key 'k_m' and access model 'f' as inputs thus producing linked elements as outcomes.

Creation of keys phase
Input:k_m and set of user elements E
Result:secret key $k_s = \{k_s, l, k_{s1},\ldots..,k_{nE}\}$
$k_s \leftarrow x_\delta + [\Delta]x_\delta$
$i \leftarrow [\Delta]q$
for i = 1 to E do
$k_{si} \leftarrow [\Delta]E$
end for
$k_s = \{k_s, l, k_{s1},\ldots..,k_{nE}\}$
return k_s

3.3.4 Decoding (s_k, c_t) → m

The decoding scheme acknowledges the private key 's_k' linked with the access model 'f' along with the cipher text 'c_t' which is linked with element set and offers a message 'm' in case it fulfills 'f'.

Decoding phase
Input: c_t and its matrix M, s_k and set of elements E
Result: Plain text P (only if elements within $s_k$fulfills the ciphertext strategy

M ← minimize the matrix M by eliminating the rows and columns isolated from the elements in E
Locate the determinant $\Delta \leftarrow D(M) \in a_r$
Estimate the vector ψ as the initial row of M^1
$c_i^{\psi_i} \leftarrow [\psi_i]c_i$
$k_i^{\psi_i} \leftarrow [\psi_i]k_i \setminus$
end for
$m = c \oplus E((E(c_t, c_i, c_i k).E(l, \sum_{i\delta E} C_i^{\psi_i}).\prod_{i\in E} E\left(d_i, k_i^{\psi_i}\right))^{\frac{1}{\rho}} \setminus$
return m

4 Performance analysis

The assessment was performed by making use of cloud simulator for which around 2000 KB text documents were gathered and assessments were conducted by making use of element based encoding scheme based on decoding the documents employing various schemes as portrayed in Table 1. The simulations were conducted with the aid of resources like core i5 processor and 80 GB RAM. Table 1 depicts the time consumed by various encoding schemes for various information sizes. The outcomes of the analysis disclose that the advanced encryption standard works quicker and it is appropriate for immense repositories as depicted in Fig. 3. The other schemes taken for assessments are DES, RC4 and Blowfish schemes.

The execution employs 160-bit elliptic curve over 512-bit fixed field and Fig. 4 portrays the execution time evaluated against advanced encryption standard and element based encoding for encoding the information portrayed in Table 2. The execution time for element based encoding is sequential in terms of leaf nodes but the advanced encryption standard does not perform better for encoding minimal volume of information. Therefore a safer model for safeguarding personal health records are constructed using element based encoding.

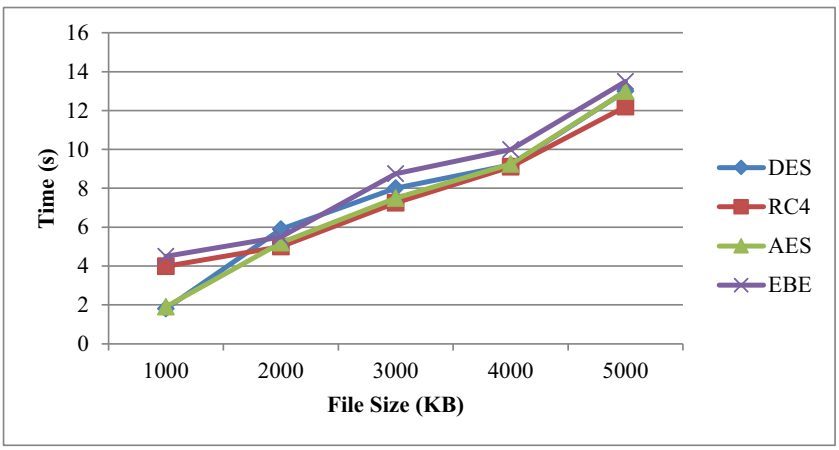

Fig. 3 Analyzing Time Needed by Different Encoding Schemes

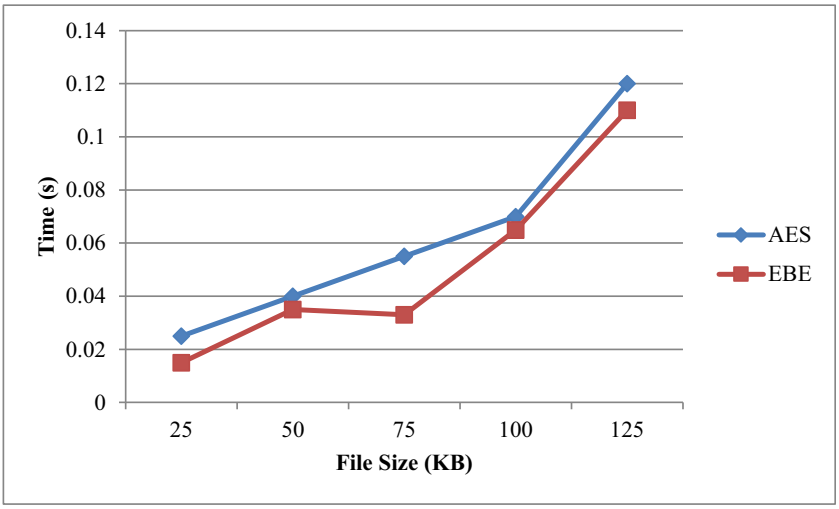

Fig. 4 Analyzing Time Needed AES and EBE for Encoding

Figure 4 portrays the elaborated estimation time-based outcomes for all the schemes. Here the restoring of user needs a minimal set of information elements allowing access model feeble. The scheme holds the minimal secret sized secret key and generating minimal sized ciphertext. Evaluated against the prevailing repealed element based encoding the key merit of the scheme is minimal in rekeying the size of the message. In order to rescind a user the utmost rekeyed size of the message is sequential based on the element count for the user secret key. It represents that the scheme is expandable than the prevailing schemes.

Therefore the element based encoding is rapid and more appropriate based on the time for creating keys, encoding and decoding operations that are sequential with a set of elements. Based on the system perspective every possessor of the information employs element based encoding for initialization, key creation, encoding and restoring where every personal domain and user domain decodes the file within minimal time. The element authority is employed for initialization, the creation of keys, user withdrawal. For 50 elements it requires the minimal time of less than 0.5 s. Therefore the element based encoding remains more expandable for execution over the personal health domain since it minimizes the difficulties in preserving keys.

Table 2 Analyzing Time Needed AES and EBE for Encoding

File Size in KB	AES	EBE
25	0.025	0.015
50	0.040	0.035
75	0.055	0.033
100	0.070	0.065
125	0.12	0.11

5 Conclusion

It is evident that verification based on hashing could offer safety as the created keys could not be possibly be rehashed. Based on the assessment it is evident that the element based encoding is far safer and it is proven that secure hash function is prominent to conflicts which could be easily broken. Therefore it is no longer safer scheme but element based encoding is not subjected to conflicts since the keys are created based on a various set of elements. The usage of element based encoding for encoding information and verification is carried out based on trials for securing the information. The work could be extended for encoding multimedia information along with nesting verification over the scattered cloud environment.

References

1. Satheesh K, Ram Kumar A (2018) Scalable and Secure Distribution of Medical Records in Cloud Computing Using Multi-Authority and Element -Based Encryption. International Journal of Research in Computer, Communicative Engineering and Technology 2:1
2. Mohan D, Rabbani SW, Mangalagowri R (2018) Data Sharing Strategy in Cloud Computing Using Element Based Encryption. International Journal of Pure and Applied Mathematics 118(22): 637–640
3. Supriya D, Talekar K, Raskar R, Chavans P (2018) Attribute Based Access Control in Personal Health Records Using Cloud Computing. International Research Journal of Engineering, Communication and Technology 5:3
4. Ali M, Abbas A, Khan U, Khan SU (2018) SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud. IEEE Transactions on Cloud Computing 1
5. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G (2018) Security and Privacy in Medical Internet of Things: A Review. Journal of Security and Communication Networks

6. Safeena C, Nagarajan VP (2018) Ensuring the Privacy of Patient Health Records (PHR) Sharing Scheme in Public Cloud by the Hybrid Encryption Cryptography. Asian Journal of Applied Science and Technology 2(4):124–131
7. Salama U, Yao L, Paik H–Y (2018) An Internet of Things Based Multi-LevelPrivacy-PreservingAccess Control for Smart Living. In: Informatics Journal 5(23)
8. Sreesaila B, Abinaya K, Swarnalatha M, Sugumar R (2018) Aadhaar Card Based Health Records Monitoring System. International Journal of Innovative Research in Computer Engineering and Technology 7(2)
9. Gokula Priya R, Madhu UP, Yuvashree M, Karthikeyan M (2018) A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing. International Journal of Engineering Research in Computer Science and Engineering 4:3
10. Abdulla R (2017) Safe Sharing of Health Records in Cloud Repositories Using HABSE. IOSR Journal of Electronics and Communication Engineering:62–67
11. Vaishnavi Y, Patel C, Vithlani S, Bhojak P (2017) Secret Distribution of Health Records in Cloud Using Attribute-Based Encryption. Int J Comput Eng Sci 7(1)
12. Pagar S, Yadhav R, Boraste S, Bairagi H (2017) Sharing of PHR on Cloud Using Attribute-Based Encryption and Access by QR – Code. International Research Journal of Engineering, Communication and Technology 4(2)
13. Zheng H, Wu J, Wang B, Chen J (2017) Modified Ciphertext-PolicyAttribute-Based Encryption Scheme with Efficient Revocation for PHR System. Journal of Mathematical Problems in Engineering
14. Mafawez A, Qawqzeh Y (2017) Proposed PHR Architecture for Saudi Arabia Health Services. J Eng Appl Sci 4(1)
15. Varshini BV, Vigilson Prem M, Geethapriya J (2017) A Review on Secure Data Sharing in Cloud Computing Environment. International Journal of Advanced Research in Computer Engineering, Communication and Technology 6(3)
16. Kumarasamy S, Asokan R (2011) An Efficient Detection Mechanism for Distributed Denial of Service (DDoS) Attack. International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) 1(5)