Journal of
Computational and Theoretical Nanoscience
Vol. 14, 4655–4663, 2017

RESEARCH ARTICLE

Securing Shared Data in E-Learning Using Three Tier Algorithm of Compression Combined Hybridized Encryption

A. Revathi[1,*], Paul Rodrigue[2], and J. Raja[3]

[1] *Research Scholar, Anna University, Chennai, Tamil Nadu, India*
[2] *Indra Gandhi College of Engineering and Technology for Women, Chennai, Tamil Nadu, India*
[3] *Adhiparasakthi Engineering College, Chennai, Tamil Nadu, India*

In e-learning design and training, the information authentication to be maintained safe and protected must be the primary priority. We might guarantee that the e-learning content formed is kept secure from the unauthorized users, particularly if it integrates with the private sector. In our intended effort we implemented the compression combined hybridized encryption that protect the shared data better than the other in e-learning. This employs two tier approach that comprises compression techniques and encryption algorithm that compress and encrypts the specified data to build it more protected in a dexterous way. Originally the given data is compressed by means of a novel lossless compression algorithm called Binary Code Indexing and Encoding (BCIE) algorithm which is preceded by the procedure of hybridized encryption that utilizes the RSA and AES encryption algorithm along with a novel algorithm called SCELL (Self-loop Code Enfilade Linked list) algorithm. Ultimately the decryption process for the specified data proceeds for the user prospect in which the compressed decrypted data is decompressed. Owing to this high security the unauthorized user is not capable to access the equivalent original data. Only the concerned owner of the data can carry out any actions on the original data and only authorized users can utilize the content. Thus our intended system surmounts the security problem in e-Learning environment.

Keywords: E-Learning, Rivest-Shamir-Adleman, Advanced Encryption Algorithm, Hybridized Encryption, Compression.

1. INTRODUCTION

While the term "e-learning" has been thrown around quite a lot in recent years, many are still unaware of what it actually means and how it can help them achieve success in both their professional and personal lives. The personal data is expanded in eLearning with the particular information about the student's background, preferences and then learning progress. Intelligent and adaptive eLearning environments utilize tracking mechanisms for serving the correct and concrete content to students and for assisting them in an effective learning progress.[2] Also, this is a premise for analyzing student's behavior, included of crossing his personal space. Social networking sites are universally employed in higher education and good practices are available for that. Anyhow, personal information allocated by the users is accumulated by social networking sites. The mobile devices' utilization leads for accumulating more data even without the students' awareness. The case of learner mobility needs even gathering location, and sometimes without the learners' awareness.[1,3]

In contemporary days Cryptography is regarded as the combination of Symmetric key algorithms[4,8] and Asymmetric-key algorithms.[9] The trustworthy management of a customer assures that the network does not study any information of the customer data.[12] For providing confidentiality and clandestine services to the data, cryptography is employed as a conventional tool.[5,6] The data are generally encrypted before saving to the network. The customer handles key management, access control, encryption and then decryption processes for ensuring data security.[13] The two accepted approaches share data securely in network storage. First, encrypt data utilizing a symmetric key and distribute that key amidst the approved users. Second, approach utilizes the authorized users' individual public key to encrypt data.[14] The public key encryption favors to be much more protected since it implicates the two different

*Author to whom correspondence should be addressed.

key combination of public and private key. More adaptability is provided by this for different applications.[15] While saving such encrypted data and recognize the issue of constructing a safety network storage service on the top of public network infrastructure in which the service provider is not thoroughly believed by the customer. In a high level, they demonstrate several architectures combining present plus un-standard cryptographic primitives for achieving our aim.[5, 7] Encryption is a special sort of cryptographic technology which implements access control through the encrypted data. The outsourced sensitive data in the network server is protected till the data owner encrypts the data prior to the uploading in the semi-trusted network.[16]

Many examples of very strong plus weak keys of the cryptography algorithms of RC2, RC6, DES, Blowfish, 3DES and AES are available. RC2 utilizes one 64-bit key. One 64-bit key is employed by DES. Triple DES (3DES) utilizes three 64-bits keys when different (128, 192, 256) bits keys are utilized by AES.[5, 17] Blowfish employs various (32-448); default 128 bits when RC6 uses various (128, 192, 256).[18] This paper describes AES plus RSA cryptographic encryption methods that are employed for protecting the data employed in the network and then restrict the information from being leaked and also ensuring the maintenance of the privacy. AES is symmetric-key encryption standard while RSA is asymmetric encryption standard.[19] AES holds the benefit of being executed in both hardware and software. The AES hardware implementation is done in three modules containing the encryption, the decryption and then the key scheduling module.[20] RSA is employed for reducing the data requirement of keys.

The out sketch of the paper has been classified such as: Section 2 contains the investigation of the assessment of corresponding works concerning recommended technique, Section 3 presents a concise thought underlying in the proposed method. Section 4 reveals the investigation of experimental outcome. At last Section 5 puts an end to the paper.

2. RELATED WORK

Ahmed Younis et al.[21] have proposed that adapting e-learning systems was to afford students educational services through electronic channels. The study focused chiefly on IT infrastructure services' impact and then IT quality on e-learning systems' usefulness perceptions. A model was suggested including five constructs. They are IT infrastructure services, information quality, service delivery quality, system quality, and also perceived usefulness. The outcome presented that IT infrastructure services holds a significant role in creating information of high quality, embellishing the e-learning system quality aspects, and augmenting service delivery quality.

Kassid Asmaa et al.[22] suggested, the security aspects are directly related to the application of a control access policy, responsible for securing interaction with agents and reinforcing it with the integration of trust. The giving work will focus on combining two access models based on RBAC model: "TrustBAC," T-SR "Dynamic RBAC with Trust-Satisfaction and Reputation for multi-agent system." The main goal here, is to develop a new model that incorporates the advantages of both models and improve the highest degree of security in the E-learning platforms based on multi-agent systems.

Stoffregen et al.[23] discussed the public administration employees' open e-learning in a recent state at the regional government level and then extracted the barriers for such learning. The results allowed informed assumptions on which obstruction will raise in the open-source e-learning technology's forthcoming utilization, specifically in open educational resources as means of learning. This study provided a contextualized obstacle framework allowing the orderly capture and comparing the challenges to assist for future studies.

Prakash Kuppuswamy et al.[24] they suggested a Hybrid Encryption System utilizing an innovative public key algorithm and also private key algorithm. A hybrid cryptosystem linked a public-key cryptosystem's convenience with a symmetric-key cryptosystem's effectiveness. Here, the suggested two ways secured data encryption system addressed the user's privacy, authentication and accuracy. The suggested systems have been employed in the Encryption plus the decryption sequence. One was public key cryptography regarding linear block cipher. The second was a simple symmetric algorithm based private key cryptography. The cryptography algorithm offered more safety and authentication while matched with other prevailing hybrid algorithm.

Emina Junuz[25] proposed a semantic e-learning environment that can use LO repository on local and global level, where ontology gives learning objects their pedagogic meaning and emphasize personalization and adaptively of learning content. Repositories that contain learning objects introduced with ontology usage were simpler to search and search results were more precise, what simplify finding adequate LO to student for learning and teacher for creating the course. Also there was a possibility that applications on automatic way used and integrate in learning object courses introduced with ontology.

3. PROPOSED METHODOLOGY

Our intended technique merely offers a valuable elucidation for defending an electronic document. This technique of security result in the e-Learning content employing the compression combined hybridized encryption (CCHE) algorithm, which facilitates the organizations to more efficiently deal with the electronic documents for continual protection. Our intended scheme includes five phases such as,

(i) Design of e-Learning Content,

(ii) Proposed Compression Combined Hybridized Encryption (CCHE),

(iii) User Authentication,
(iv) Proposed Compression Combined Hybridized Decryption (CCHD),
(v) Retrieval of the original e-Learning content.

An outline of the entire process is illustrated in Figure 1.

3.1. Design of E-Learning Content

Various apparatus for designing and implementing E-content are offered in the market. Several packages range from easy to use to the complicated ones that requires the skilled computer programmers or the developers of the E-content. Another difficulty with these packages is that majority of them must be acquired and licensed which can be an impediment and has an additional cost to be deliberated for the instructors and the beginners who are willing to build up or utilize the E-content.

It can be a booming technique that the developer of an E-Learning content seems to be one of the course instructors whom might not be an expert in using computers and authoring software packages that can be employed for emerging the E-Learning content. The usage of obtainable tools and software packages like Office software package can make it simpler for the non-expert developers and the users of E-Learning.

Even though there may be a few features in the other electronic authoring packages which are better to this package, or ideal to few users; but the common use of this proposed technique among computer users can make the development and use of E-Content which may be text file or image file which is used to build over previous expertise. The management of the e-Learning content is governed by the owner of the data who is considered as the admin.

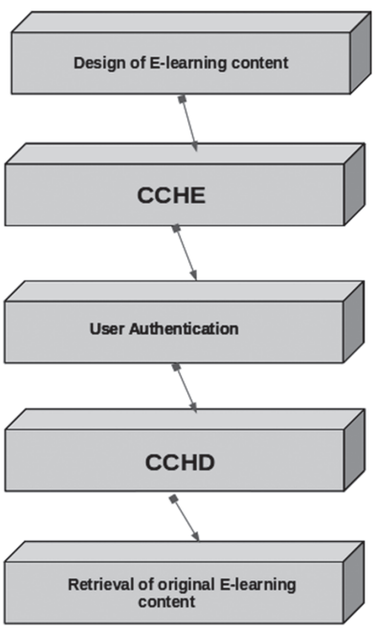

Fig. 1. Block diagram for procedure of the proposed method.

3.1.1. Preparation of Learning Objects

In order to prepare educational contents relating on different sections of knowledge, to be used again in learning process and teaching and to be available it is necessary to transform the content to learning objects. Learning object (LO) is main unit of electronic educational content that gets created with maximization different use cases and simpler distribution and re-usage, idea similar to object-oriented paradigm.

Description of objects is more effective as each single learning object used in the proposed technique differs from other learning object due to the content included in it. The learning objects are divided based on the related content based on the topic selected. In our proposed method various learning objects are created on different fields of knowledge that are related to the new trends in the information technology. For example the learning objects used includes the topics of cloud computing, data mining, Image Processing and so on.

In our proposed effort the input to be preserved by the owner accepts the input as the text and image file type which is the divided learning object. The owner of the e-Learning content can pick the large number of text and image files that can be protected in the e-Learning environment which is available in the form of learning object.

3.2. Proposed Compression Combined Hybridized Encryption (CCHE)

3.2.1. Compression Technique

Compression is the process of shrinking the size of the data with the aid of a program that employs an algorithm or in that case any procedural formula. The compression process may be lossy or lossless in nature. When we decompress a file that is compressed with Lossless compression, it will be restored to its original state without any bits loss. When we decompress a file that is compressed with Lossy compression, it will be restored to its original state with some loss of bits. The compression mentioned in this procedure must not be taken as a data de-duplication procedure. De-duplication is a type of compression that looks for redundant chunks of data in the file storage system and replaces each duplicate chunk with a pointer to the original so that the pointer access will point out to the actually stored data.

The compression approach used in this procedure is Binary Code Indexing and Encoding (BCIE) algorithm. It is a Lossless compression algorithm. The original text and image files are chosen by the owner of the data was initially compressed by means of the proficient. As the Compression before encryption also faintly raises the sensible resistance against differential crypt-analysis (and particularly other attacks) if the attacker can only control the

uncompressed plain text, as the resulting output may be hard to deduct. In circumstances such as when the content owner does not hope the network operator, he will not provide the cryptographic key which was employed to encrypt the data. Hence for expanding the network utilization; the network owner is enforced to compress the data then it is encrypted. Owing to the above payback of compression before the encryption we choose the compression approach primarily in our intended effort.

3.2.1.1. Binary Code Indexing and Encoding (BCIE) Compression Algorithm. Binary Code Indexing and Encoding (BCIE) algorithm is a multi pass algorithm and it compresses any given data by identifying the most prominently occurring adjacent set bytes in the data and replacing all instances of the adjacent set bytes with a byte that was not in the original given data (unexploited byte). The Binary Code Indexing and Encoding algorithm repeats this process until no further compression is possible. This may be because of absence of prominently occurring adjacent set bytes or may be because of lack of unemployed bytes to represent the prominently occurring adjacent set bytes. The algorithm writes out the table of dual substitutions before the packed data.

3.2.1.1.1. BCIE Algorithm–Compression Pseudo Code.

```
Read file
While not end of file
    Read next block of data into buffer memory and
      enter all adjacent sets in hash table with counts of
        their occurrence
    While compression possible
      Find most frequent adjacent set bytes
      Replace pair with an unexploited byte
    If substitution deletes an adjacent set bytes from
      buffer, decrease its count in the hash table
    If substitution adds a new adjacent set bytes to the
      buffer, increase its count in the hash table
    Add adjacent set bytes to adjacent set bytes table
End while
    Write adjacent set bytes table and packed data
End while
```

3.2.1.1.2. BCIE Algorithm–Expansion Pseudo Code.

```
Read file
While not end of file
    Read adjacent set bytes table from input
    While more data in block
      If stack empty, read an unexploited byte from
        input
        Else pop an unexploited byte from stack
      If an unexploited byte in table, push pair on stack
        Else write an unexploited byte to output
    End while
End while
```

The main advantage of the BCIE algorithm is that it maintains the file size as a constant attribute. This feature of BCIE is maintained even with random data types and also with compressed data types. Lastly, the outcome of the Binary Code Indexing and Encoding (BCIE) compression algorithm yields the compressed format of the text content and image files opted for e-Learning.

3.2.2. Hybridized Encryption Algorithm (HE)

Our intended Compression Combined Hybridized Encryption (CCHE) uses the hybridized algorithm RSA and AES encryption algorithm along with a novel algorithm called SCELL (Self-loop Code Enfilade Linked list) algorithm. The output of the BCIE compression algorithm which is in the compressed format of the text files and the image files are given as the input for the Hybridized encryption algorithm. Our hybridized algorithm utilizes the RSA encryption algorithm for the encryption of the compressed data that can include both text and image files. The private key generated in the RSA algorithm is given into the SCELL algorithm for further dual key encryption. Then the private key generated in the SCELL algorithm is encrypted by means of the AES encryption algorithm. The entire proposed architecture is illustrated below in Figures 2 and 3.

3.2.2.1. RSA Algorithm (Encryption). RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually

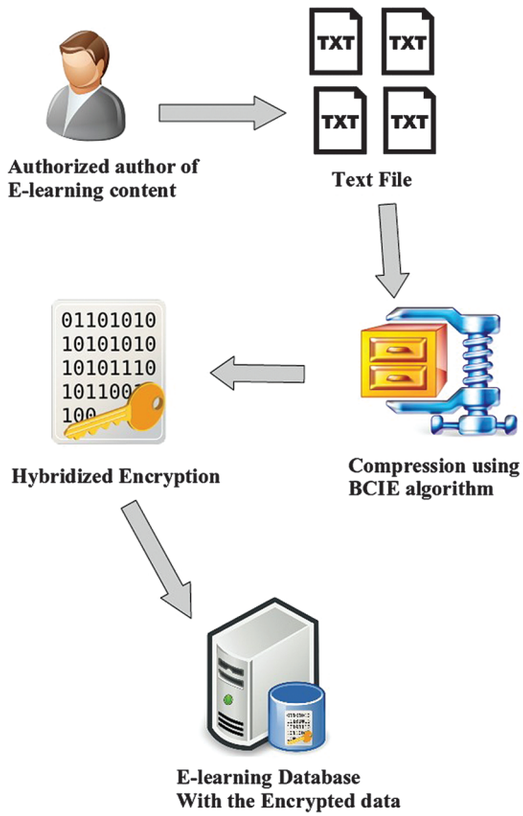

Fig. 2. Proposed architecture showing the encryption and storage part.

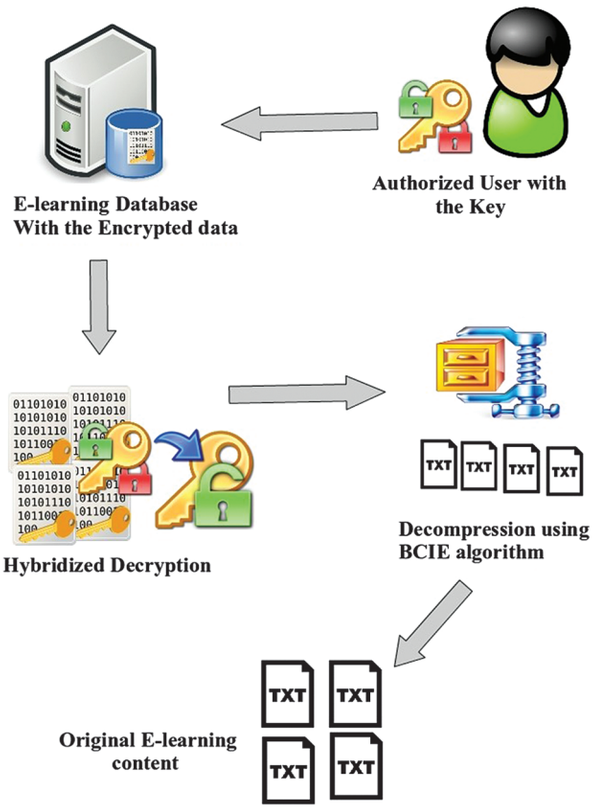

Fig. 3. Proposed architecture showing the decryption and data retrieval part.

means that it works on two different keys i.e., *Public Key* and *Private Key*. As the name describes that the Public Key is given to everyone and Private key is kept private. The RSA algorithm works as follows:

- Choose any two prime numbers p and q
- Compute the modulus in which the arithmetic will be done: $n = pq$

(*Note: This n is the public key*)

- e is an integer but not necessarily a factor of n
- Pick a public encryption key $e \in Zn$

(*Note: This public key is made up of n and e*)

- $1 < e < \Phi(n)$

(*Note:* $\Phi(n)$ *is Euler's Totient function*)

- $\Phi(n) = (P-1)(Q-1)$

(*Note:* $\Phi(n)$ *is calculated*)

- $d = (k * \Phi(n) + 1)/e$

(*Note: d is the Private key*).

Now we have our Private and Public key. Using this we can perform Encryption and Decryption of any message.

- Encryption of message m: $c = me \ modN$
- Decryption of crypto message c: $m = cd \ modN$

In our process the E-learning content is Encrypted using the RSA algorithm. RSA algorithm is an Asymmetric key algorithm. The main reason for using RSA algorithm as the first encryption step is due to its key length factor which depends on the number of bits in the modulus n where $n = pq$ (Theblocksizeisvariable). The cipher type is Asymmetric block cipher. The Private key generated is subjected to a secondary level of encryption using SCELL algorithm.

3.2.2.2. SCELL Algorithm (Secondary Encryption). The proposed SCELL (Self-loop Code Enfilade Linked list) algorithm is devised as an additional security algorithm which takes the Private key and gives it a random gibberish code which will not be taken into the AES algorithm encryption and will act as a temporary cover to the real encryption process. The entire operations of SCELL algorithm is presented in the form of a pseudo code for a outlier understanding.

3.2.2.2.1. SCELL algorithm–Encryption Pseudo Code.

Step 1: Read the Private key
Step 2: Converts the Private key to binary format
Step 3: Assign DNA bases to the binary format and Replace DNA bases with the numbers given in the reference DNA sequence
Step 4: Transmit the encrypted Private key.

3.2.2.2.2. SCELL Algorithm–Decryption Pseudo Code.

Step 1: Convert the encrypted Private key
Step 2: Replace the numbers with DNA bases given in the reference DNA sequence
Step 3: Replace DNA bases with the binary numbers
Step 4: Convert the binary format back into Private key.

3.2.2.3. Private Key Encryption Using AES. AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. The AES algorithm comprises of three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively.

3.2.2.3.1. AES Algorithm-Pseudo Code.

```
Cipher (byte in[16], byte out[16], key_array round_key[Nr+1]) begin
byte state[16];
state = in;
AddRoundKey (state, round_key[0]);
for i = 1 to Nr − 1 stepsize 1 do
SubBytes (state);
ShiftRows (state);
MixColumns (state);
AddRoundKey (state, round_key[i]);
end for
SubBytes (state);
ShiftRows (state);
AddRoundKey (state, round_key[Nr]);
end
```

The output with the encrypted text content by means of the RSA and encrypted private key is hoarded to the e-Learning

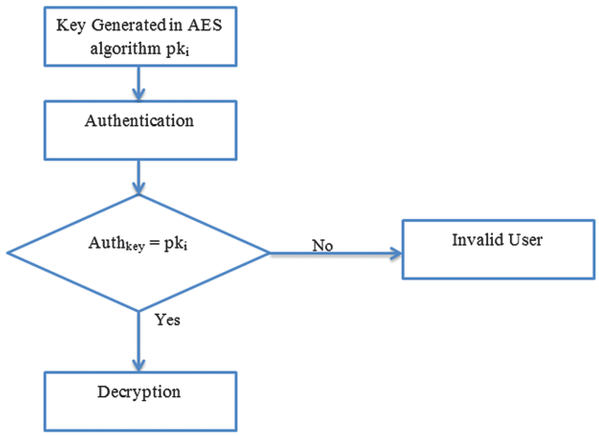

Fig. 4. Steps for the authentication process.

database. Thus the encrypted form of the text and private is hoarded firmly in the e-Learning environment.

3.3. User Authentication

Authentication is the process by where the system authenticates the identity of a User who desires for accessing it. As the Access Control is generally depends upon the identity of the User which request the access to a resource, Authentication is vital for the effectual Security.

The above Figure 4 illustrates the process of authentication carried out. The Authentication process proceeds as any user tries to decrypt the data. The encrypted content of the e-learning environment is protected by the key used in the AES algorithm. The owner of the e-learning data only can share the original key value to the authorized users so that they can only decrypt the data which includes the text and image files of the e-learning environment. Other unauthorized users without the key value provided the admin cannot de-crypt and read the e-learning content. Thus secured data in the e-Learning database can access merely by the allowed users holding the exact key. The users merely offering the exact matching keys can continue for the decryption process.

4. RESULTS AND DISCUSSION

In this segment, we exhibit few experimental outcomes of our intended two tier algorithm for protecting the shared data in the cloud. Our key effort is examining the performance of the intended effort and monitors how it varies with few other conventional algorithms for dissimilar data values.

4.1. Performance Analysis

The functioning of the intended technique is assessed depending upon the time employed during the encryption process for text file by dissimilar amalgamation of hybridized cryptographic algorithms such as the hybridized algorithm of ECC AES and the hybridized algorithm of ECC DES with our intended hybridized algorithm which comprises RSA and AES.

Table I. Performance of proposed compression combined hybridized encryption technique with the existing techniques for 1325 bytes.

1325 bytes	Proposed	E1 (ECC-AES)	E2 (ECC-DES)
Data encryption time	0.116866	0.252568	0.232982
Key encryption time	0.038882	0.041661	0.048582
Key decryption time	0.019551	0.023207	0.033169
Data decryption time	0.055591	0.347373	0.342952
Compression time	0.105611	0.105848	0.105759
Decompression time	0.081367	0.083395	0.082257
1st AlgmKey_G_Time	0.016297	0.032502	0.019415
2nd AlgmKey_G_Time	0.006572	0.00678	0.007392

4.1.1. Discussion

Table I exhibits the performance of the intended compression combined hybridized encryption technique with the conventional techniques in terms of Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2nd AlgmKey_G_Time for 1325 bytes metrics. While observing the comparison table, Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2nd AlgmKey_G_Time of our intended technique is 0.116866, 0.038882, 0.019551, 0.055591, 0.105611, 0.081367, 0.016297 and 0.006572 respectively. It is indeed less when related with the conventional technique. Therefore our suggested technique yields superior outcomes than the conventional approaches by generating the minimum time effect than the conventional one with high security concern. The comparison graph has been exposed in the Figures 5 and 6.

4.1.2. Discussion

The illustrated Figures 5 and 6 epitomizes the graph which proves that the time taken in encryption process for text file by dissimilar compression combined hybridized algorithms such as ECC-AES and ECC-AES related with the intended compression combined hybridized RSA-AES

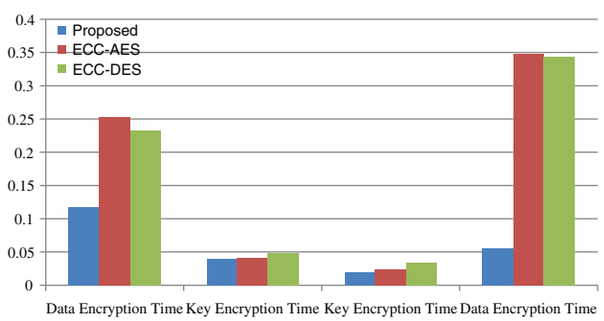

Fig. 5. Comparison of the proposed method with the existing method.

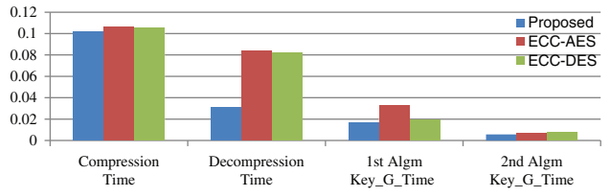

Fig. 6. Comparison of the intended method with the conventional method for 1325 bytes size.

algorithm. This graph evidently implies that our intended technique need less time for encryption process for 1325 byte of text data.

4.1.3. Discussion

Table II exhibits the performance of the intended compression combined hybridized encryption technique which is related with the conventional techniques based on Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2nd AlgmKey_G_Time for 1325 bytes metrics. When seeing the comparison table, Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2nd AlgmKey_G_Time of our proposed technique is 0.157732, 0.038618, 0.019263, 0.077523, 0.160586, 0.110297, 0.032298 and 0.006449 respectively. It is indeed less when related with the conventional technique. Therefore our intended technique yields superior outcomes than the conventional techniques by generating the minimum time effect than the conventional one with high security concern. The comparison graph is illustrated below in Figures 7 and 8.

4.1.4. Discussion

The illustrated Figures 7 and 8 epitomizes the graph which proves that the time taken in encryption process for text file by dissimilar compression combined hybridized algorithms such as ECC-AES and ECC-AES related with the intended compression combined hybridized RSA-AES algorithm. This graph evidently implies that our intended

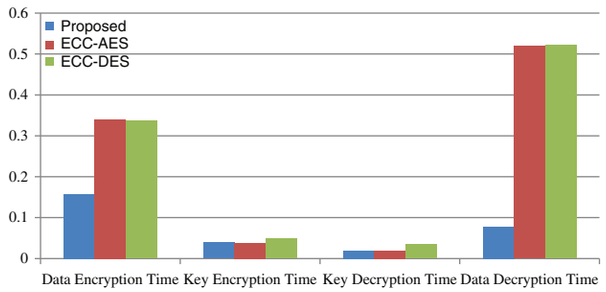

Fig. 7. Comparison of the intended with the conventional technique for 2264 bytes.

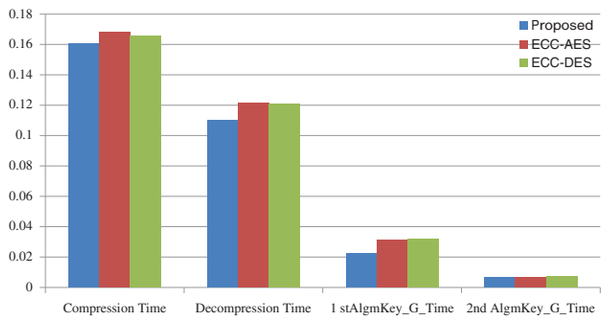

Fig. 8. Comparison of the intended technique with the conventional technique for 2264 bytes.

technique need less time for encryption process for 2264 bytes of text data.

4.1.5. Discussion

Table III exhibits the performance of the intended compression combined hybridized encryption technique which is related with the conventional techniques in terms of Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2nd AlgmKey_G_Time metrics for 4216 bytes. When seeing the comparison table, Data Encryption Time, Key Encryption Time, Key Decryption Time, Data Decryption Time, Compression Time, Decompression Time, 1st AlgmKey_G_Time, 2ndAlgmKey_G_Time of

Table II. Performance of the intended compression combined hybridized encryption technique with the conventional techniques for 2264 bytes.

2264 bytes	Prop	E1 (ECC-AES)	E2 (ECC-DES)
Data encryption time	0.157732	0.34012	0.336219
Key encryption time	0.038618	0.038194	0.048226
Key decryption time	0.019263	0.019095	0.034252
Data decryption time	0.077523	0.519131	0.521595
Compression time	0.160586	0.168232	0.165641
Decompression time	0.110297	0.121089	0.12091
1st AlgmKey_G_Time	0.032298	0.021344	0.031647
2nd AlgmKey_G_Time	0.006449	0.005584	0.007425

Table III. Performance of the intended compression combined hybridized encryption method with the conventional method for 4216 bytes.

4216 bytes	Proposed	E1 (ECC-AES)	E2 (ECC-DES)
Data encryption time	0.22778	0.533971	0.543603
Key encryption time	0.030218	0.040027	0.049178
Key decryption time	0.01893	0.019896	0.033985
Data decryption time	0.12649	0.855953	0.850043
Compression time	0.287441	0.299094	0.39117
Decompression time	0.105014	0.198613	0.200208
1st AlgmKey_G_Time	0.012676	0.013216	0.015775
2nd AlgmKey_G_Time	0.005719	0.006994	0.007574

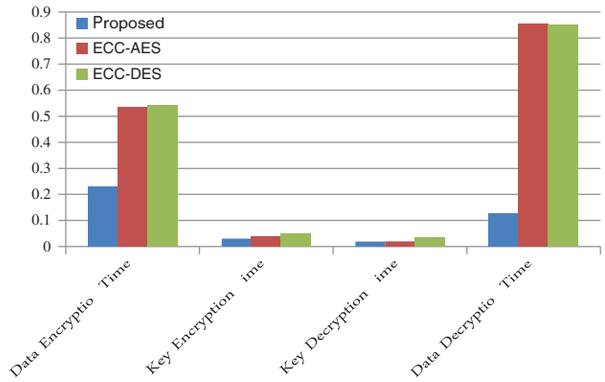

Fig. 9. Comparison of intended method with the conventional technique for 4216 bytes.

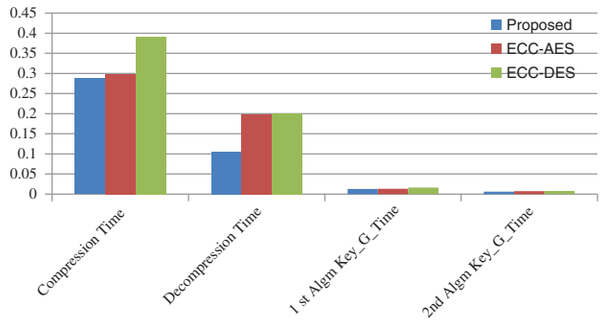

Fig. 10. Comparison of the intended with the conventional technique for 4216 bytes.

our proposed technique is 0.22778, 0.030218, 0.01893, 0.12649, 0.287441, 0.105014, 0.012676 and 0.005719 respectively. It is indeed less when related with the conventional technique. Hence our intended technique yields better outcomes than the conventional techniques by yielding the minimum time effect than the existing one with high security concern. The comparison graph is illustrated below in the Figures 9 and 10.

4.1.6. Discussion

The illustrated Figures 9 and 10 gives the graph which proves that the time taken in encryption process for text file by dissimilar compression combined hybridized algorithms such as ECC-AES and ECC-AES related with the intended compression combined hybridized RSA-AES algorithm. This graph evidently implies that our intended technique need less time for encryption process for 4216 bytes of text data.

5. CONCLUSION

The expounded effort proposes file security in e-Learning environment. Where the cost and user friendliness are the two main benefit of e-Learning environment, there includes noteworthy security concerns that ought to be addressed while deliberating the moving critical content and sensitive data to public and shared e-Learning environments. Compression and hybridized encryption of large text data yields a proficient method of handling it. Amalgamation of these approaches lessens the size initially and then builds the reduced size tenable, which takes less time. These techniques can be valuable in hoarding memory and data transfer. The intended method yields superior outcomes by pooling the LZW method, which is a lossless compression, with the novel hybridized encryption algorithm. It is hard for the third party to split the system even with its simple, simple to understand the architecture. Files can be uploaded in the encrypted form and by employing the concept of keys file can be downloaded. Thus our proposed technique enables the secure environment in the e-Learning.

References

1. Venkatapathy Subramanian, Towards business process management based workplace e-learning, *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*, IEEE **(2016)**, pp. 555–557.
2. I. Kamsa, R. Elouahbi, F. El Khoukhi, T. Karite, and H. Zouiten, Optimizing collaborative learning path by ant's optimization technique in e-learning system, *2016 15th International Conference on Information Technology Based Higher Education and Training (ITHET)*, IEEE **(2016)**, pp. 1–5.
3. M. Ivanova, G. Grosseck, and C. Holotescu, Researching data privacy models in eLearning, *2015 International Conference on Information Technology Based Higher Education and Training (ITHET)*, IEEE **(2015)**, pp. 1–6.
4. S. Abu-Dawood, The cognitive and social motivational affordances of gamification in e-learning environment, *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*, IEEE **(2016)**, pp. 373–375.
5. A. Abid, IlhemKalle, and M. B. Ayed, Teamwork construction in E-learning system: A systematic literature review, *2016 15th International Conference on Information Technology Based Higher Education and Training (ITHET)*, IEEE **(2016)**, pp. 1–7.
6. Sumeet Bajaj and RaduSion, *IEEE Transactions on Knowledge and Data Engineering* 26, 752 **(2014)**.
7. Priyanka Rajagouda Pradhan and R. B. Kulkarni, Secure e-learning using data mining techniques and concepts, *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, IEEE **(2016)**, pp. 1498–1501.
8. Y.-Q. Zhang and X.-Y. Wang, *Information Sciences* 273, 329 **(2014)**.
9. W. Liu, Z. Xie, Z. Liu, Y. Zhang, and S. Liu, *Opt. Commun.* 335, 205 **(2015)**.
10. B. Norouzi, Seyed Mohammad Seyedzadeh, SattarMirzakuchaki, and Mohammad Reza Mosavi, *Multimedia Systems* 20, 45 **(2014)**.
11. Kanyasree Mustafi, Nazimuddin Sheikh, Tapan Kumar Hazra, ManiratnaMazumder, Ishan Bhattacharya, and Ajoy Kumar Chakraborty, A novel approach to enhance the security dimension of RSA algorithm using bijective function, *2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE **(2016)**, pp. 1–6.
12. Yogendra Kumar Jain and Pramod B. Gosavi, Email security using encrption and compression, *2008 International Conference on Computational Intelligence for Modelling Control and Automation*, IEEE **(2008)**, pp. 136–139.
13. Vishwanath S. Mahalle and A. K. Shahade, Enhancing the data security in cloud by implementing hybrid (Rsa&Aes) encryption algorithm, *2014 International Conference on Power, Automation and Communication (INPAC)*, IEEE **(2014)**, pp. 146–149.

14. Nasrin Khanezaei and ZurinaMohdHanapi, A framework based on RSA and AES encryption algorithms for cloud computing services, *2014 IEEE Conference on Systems, Process and Control (ICSPC)*, IEEE **(2014)**, pp. 58–62.
15. Amit Pande, PrasantMohapatra, and J. Zambreno, *IEEE MultiMedia* 20, 50 **(2013)**.
16. Garima Bhargava and AbhishekMathur, Enhanced spread spectrum image watermarking with compression-encryption technique, *2014 IEEE 8th International Conference on Intelligent Systems and Control (ISCO)*, IEEE **(2014)**, pp. 256–261.
17. W. Fangfang, W. Huazhong, C. Dongqing, and P. Yong, Substation communication security research based on hybrid encryption of DES and RSA, *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE **(2013)**, pp. 437–441.
18. Swapna B. Sasi and N. Sivanandam, *Indian Journal of Science and Technology* 8, 216 **(2015)**.
19. A. Masmoudi and W. Puech, *IET Image Processing* 8, 671 **(2014)**.
20. Aswathi Mohan and M. Ramkumar Raja, Delay optimization in advanced encryption standard architecture 1, 59 **(2014)**.
21. Ahmed Younis Alsabawy, A. Cater-Steel, and J. Soar, *Computers in Human Behavior* 64, 843 **(2016)**.
22. E. Baralis and L. Cagliero, *Journal of Latex Class Files* 13, 307 **(2014)**.
23. J. D. Stoffregen, Jan M. Pawlowski, E. Ras, E. Tobias, SnezanaŠćepanović, D. Fitzpatrick, and T. Mehigan, *Technological Forecasting and Social Change* 111, 198 **(2016)**.
24. Prakash Kuppuswamy and Saeed QY Al-Khalidi, *International Journal of Information and Computer Security* 6, 372 **(2014)**.
25. E. Junuz, *Procedia Social and Behavioral Sciences* 1, 824 **(2009)**.

Received: 17 March 2017. Accepted: 25 April 2017.