Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.032222
Article

Tech Science Press

check for updates

Enhanced Rsa (Ersa): An Advanced Mechanism for Improving the Security

S. Castro[1,*] and R. PushpaLakshmi[2]

[1]Karpagam College of Engineering, Coimbatore, 641032, Tamil Nadu, India
[2]PSNA College of Engineering And Technology, Dindigul, 624622, Tamil Nadu, India
Corresponding Author: S. Castro. Email: castros9747@gmail.com
Received: 10 May 2022; Accepted: 08 September 2022

Abstract: Cloud computing has become ubiquitous in our daily lives in recent years. Data are the source of technology that is generated hugely by various sources. Big data is dealing with huge data volumes or complex data. The major concern in big data is security threats. Security concerns create a negative impact on the user on the aspect of trust. In big data still, security threats exist as commonly known as DDOS (Distributed-Denial-of-Service) attacks, data loss, Inadequate Data Backups, System Vulnerabilities, and Phishing as well as Social Engineering Attacks. In our work, we have taken the data loss and Inadequate Data Backups issues into consideration. We analyze that RSA (Rivest, Shamir, & Adleman) is the most secure cryptography mechanism. In cloud computing, user authentication is the weaker section to be secured. Generally, the cryptography mechanism is done in the authentication section only. We implemented our new idea of registration with selected images and pins for processing RSA. By valid authentication approval earned by the proposed mechanism, the user is allowed to use the cloud database, encryption, decryption, etc. To prove the efficiency level of our proposed system, a comparison work is conducted between DSSE (Digital Signature Standard Encryption) and EFSSA (Efficient framework for securely sharing a file using asymmetric key distribution management). The experimental work is carried out and the performance evaluation is done using encryption time and decryption time analysis, throughput, and processing time. On this observation, the security level attained by ERSA is far better in comparison to DSSE and EFSSA with the maximum throughput attained by the proposed E-RSA being 500 Mb/Min and encryption time of 3.2 s, thus ensuring the user trust in using the cloud environment.

Keywords: Cloud computing; encryption; decryption; file sharing; RSA; key generation

1 Introduction

In our day-to-day lives, scientific inventions are evolving all around the world. Data or information is a kind of communication mode. For data sharing, several technologies have emerged, including mobile, cloud computing, etc. The data is of various types, such as emails, text, Boolean, decimal, locale, number, date,

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

images, videos, etc. These data types are mainly used by mobile phones through the internet. Data may have sensitive information, which requires a high-security level. Compared to images and videos, emails, text, Boolean, decimal, locale, number, and date consume minimum energy as well as storage. For handling this data, several technologies have evolved in a wider manner. "Big data" is a larger or more complex data set. "Big data" is the process of extracting information from a huge database. Analysis of data is helpful in developing new inventions, businesses, science, preventing diseases, crime prevention, and so on. Big data is obtained from a variety of sources, the most prominent of which is social media. In modern society, social media has a greater impact. This results in the generation of huge volumes of data, which is considered to be increasing in the future also. The big data consists of text, images, videos, etc., which are collected from various sources. Big data is connected to three factors, such as;

- Volume
- Velocity
- Variety

The amount of data which is huge, unstructured and low-density data, etc., is defined in terms of volume. Velocity is the transmission range that determines the data received and acted on. Variety determines the data types, such as structured, unstructured, and semi-structured data. Structured data is traditional data that fits perfectly in a relational database. The unstructured and semi-structured data includes text, images, audio, and video, which require additional resources to process. The process results in the extraction of meaningful data, which supports metadata. Big data workflow has three steps, such as integrating, managing, and analyzing. Integration is the process of bringing together the overall collected information from various sources. Managing is the process of storing data that has desired processing requirements and engines on an on-demand basis. The analysis is the mechanism of getting data clarity. It should be in visualization form or any data model in a structured form.

1.1 Security Issues in Big Data

Privacy and Confidentiality: Most cloud services for handling large amounts of data are provided by a third-party vendor. There is a need to guarantee data access to the data owner. The risk of cloud personnel accessing sensitive data is one of the major potential threats in the cloud environment. Hence, by utilizing highly effective privacy policies and procedures, data in the cloud will be safe at any level and confidentiality should be ensured for the data owners.

Data Integrity: Once the data is stored in the cloud, there is no more info for the user. Either the stored data is accessed by anyone else or may be edited. That is no idea about what happens to certain data, and ensuring data integrity is a vital one. There is a need for updated integrity mechanisms such as particulars like where the data is hosted, when, its originality, etc.

Data Location and Relocation: As cloud services are remote services that have a higher degree of data mobility, there is no acknowledgment of the data location because the data owner once stored the data. There is a quality policy or agreement between the cloud provider and the user that needs to be followed about the data storage location. In any condition, the user needs to store in any other specified location for action to be taken properly. Another major problem is transforming data from one place to another so there won't be any missing data leakage. Hence, the data have highly sensitive information, and there is an enhanced policy that needs to be done with the provider and user.

Data Availability: Cloud computing services are used by a wide range of either a single person or organization. The major issue is data availability, as the data are chunked and stored in different locations or different Clouds.

Storage, Backup, and Recovery: In a cloud computing environment, storage flexibility is very important. It is essential for the cloud provider must have AID (Redundant Array of Independent Disks) storage systems. It facilitates several copies of multiple independent servers.

Cyber security and privacy are the major concern in the handling of this big data. Cloud computing is one of the popularly emerging technology for handling big data. The increasing cost factors and demand for reliable services make cloud computing ahead in the industry. Cloud computing is distributing computing that enables computing resources like applications, storage, servers, networks, and services for managing big data. Cloud services are remote services that process and store big data through the internet. There are three kinds of cloud services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). There are four cloud deployment models public cloud, private cloud, hybrid cloud, and community cloud. The cloud locations are independent and its security principles are confidentiality, integrity, and availability. There are several cloud providers are evolved, among which the industrial giants are Amazon Web Service (AWS), Microsoft Azure, Google Cloud Platform, IBM Cloud Services, Adobe Creative Cloud, Kamatera, VMware, and Rackspace. However, cloud computing has several significant features in the same manner as the problems also. Some of the commonly known issues are load balancing, scheduling, and security. The user using the cloud relies on the cloud service providers for storing their sensitive data. Data security is vital in protecting user privacy. Most of the existing methods compromise the authentication mechanism easily. Cloud security is a huge topic that combines several security policies, technologies, and controls for protecting the data as well as infrastructures from possible attacks. In this way, cloud security can be achieved by a technical term known as cryptography. It consists of two processes such as encryption and decryption. Encryption is the process of converting plain text into ciphertext. Decryption is the process of changing the ciphertext into the original text using the key. An authenticated key is generated and disclosed to the user.

This paper is organized as follows Chapter 1 has the introduction, and Chapter 2 has the related work with cloud security issues. Chapter 3 has our proposed work contribution along with a detailed description of the proposed architecture, principle, and workflow. Chapter 4 has the experimental results and finally, Chapter 5 has the conclusion part.

2 Related Works

Ocansey et al. [1] proposed their work on preventing sensitive information leakage in cloud computing. Generally, the data owner stores the file in the cloud and uses it whenever it's necessary by providing proper authentication credentials. In this work, the author considers the search complexity of the cloud as the files are encrypted and stored. For this, the author developed dynamic searchable encryption schemes that contain dynamic symmetric searchable encryption (DSSE) with forwarding privacy. This method results in an effective way toward the security level of cloud computing. Pradeep et al. understood the importance of security during file sharing. Most of the challenges in the cloud have never been addressed by the existing methods. Sharing files through any device has the possibility of Identity Access Management (IAM). This allows high jackers and intruders to easily access the file from the cloud. Pradeep et al. [2] proposed an efficient framework for securely sharing a file using asymmetric key distribution management (EFSSA). In comparison, the proposed scheme shows better results than the ElGamal and Paillier methods.

Gupta et al. [3] discussed the privacy and security issues in the handling of multimedia data. The author stated that most of the multimedia data are consumed through mobile usage and Social media. These big data are effectively handled using cloud technology. In this analysis, the author described detail several open questions about the variety of security and privacy issues of multimedia big data in mobile and cloud computing. Jain et al. [4] proposed enhancement of the map-reduce layer in cloud computing. In this

work, the author addressed the security issues in handling social networks and mobile device data. Here big data privacy and security are enhanced by implementing the SMR model. This methodology improves the performance of the security and privacy layer between HDFS (Hadoop Distributed File System) and MR Layer (Map Reduce) by a new proposed Secured Map Reduce (SMR) Layer.

Alouneh et al. [5] identify an effective approach for handling big data. The author's proposed work is an effective classification approach consisting of two different tiers. In the first tier, classification is done according to its structure. The second tier influences its security, volume, variety, and velocity based on GMPLS (Generalized Multiprotocol Label Switching) and MPLS (Multiprotocol Label Switching) networks. The work improves by minimizing the data evaluation and processing time on big data. R. Mudgal and M. K. Bhatia [6] proposed cloud security using the Splitting Technique. In the cloud, the data is from a different location and is stored in another location. Due to the security issue, the exact location will not be leaked. The author states that cloud privacy is based on both hardware and software, which are present in the cloud architecture. In this work, the author increased the security level by using a multiple-core processor. To achieve reliability, the split algorithm is used. It splits the file into several fragments, then encodes and stores it in the cloud. It achieves effective results in the aspect of reliability in the cloud environment. Belguith et al. [7] analysis in his work shows that in cloud computing, cryptography is done mostly on the user side. The loss of user control leads to various security issues and unprecedented usage demand. The data is stored on the remote server and most of the work applies attribute-based cryptography to the outsourced data. For this, the author analyses various attribute-based cryptographic techniques and their limitations.

Kaaniche et al. [8] proposed PHOABE (Policy Hidden Outsourcing Attribute-Based Encryption) for a secured cloud mechanism. In this work, the author considers the security level of data sharing between dynamic groups of members. For this, the author proposed a Securely Outsourcing Multi-Authority Attribute-Based Encryption with Policy Hidden to assist with IoT. PHOABE consists of a multi-attribute authority ABE scheme. The performance of PHOABE is examined under the random oracle model, which results in an effective result in IoT-constrained environments. Xiong et al. [9] worked towards the improvement of edge computing. When a huge number of files are uploaded, there is a network delay and security issues. The author addressed the privacy protection issue by proposing an efficient ciphertext-policy attribute-based encryption (CP-ABE) scheme. The three main features of this mechanism are hidden policy, direct revocation, and verifiable outsourced decryption. The performance of CP-ABE with the Diffie–Hellman assumption and the Decisional Bilinear Diffie–Hellman assumption improves the security of outsourced data.

Zhong et al. [10] introduce a multi-authority attribute-based encryption access control scheme with policy hidden. The proposed work is the combined architecture of fuzzy fine-grained access control and cipher text policy attribute-based encryption (CP-ABE). The main intentions of this work are to solve user revocation and protect data privacy and access policy privacy. Zhao et al. [11] concentrated their work on building a secure cloud system for users who outsource or share their sensitive information. The main motto of this work is to improve security in data sharing and maintain data confidentiality. The author proposed Realizing Fine-Grained and flexible access control to outsourced data with attribute-based cryptosystems. This is a combined approach of attribute-based encryption (ABE) and attribute-based signature (ABS). In the Standard Model, Ge et al. [12] created a short and efficient expressive attribute-based signature. Under the existing method, an expressive attribute-based signature scheme is proposed with efficiency in the aspect of computation cost and signature size. Liu et al. [13] identified the anonymous authentication problem by proposing an attribute-based signature (ABS). This approach is very effective with small computation tasks. The security model combines the users' signing key, which protects the privacy policy of the user while outsourcing.

3 Proposed Work Contributions

Our main motto of this research is to enhance the level of privacy and security using the cryptography mechanism in big data platforms [14]. As per our analysis and stated above several issues are based on the authentication before using the cryptography mechanism. It is done at the user end and thus motivated to improve the secureness using a double encryption process. The principle of this mechanism is simply improving privacy during account creation. It can be done by creating a new account or through login with google, Facebook, or linked it. The registration process is the same with one advancement such as implementing using images and numerical methods. The entire proposed mechanism is explained in detail in the upcoming sections.

3.1 Proposed Methodology

The proposed mechanism has two sections Fig. 1 enhancing the security level in the user registration process and the implementation of RSA-based cryptography. RSA is one of the popular secured mechanisms used in cloud technology, but using this several existing mechanisms face security issues. This sparks our intention in improving the security level at authentication.

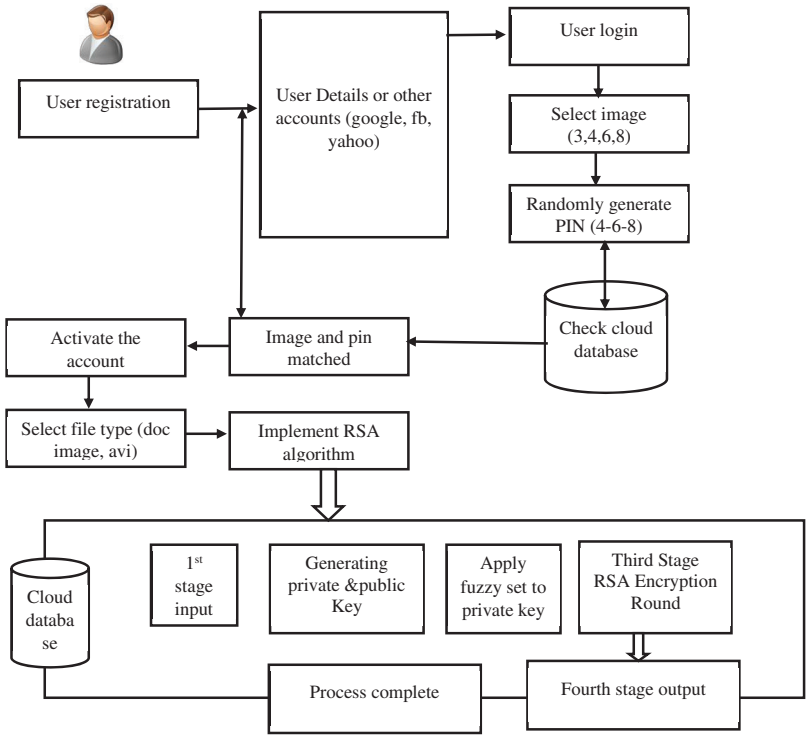

Figure 1: Proposed ERSA architecture

As mentioned, our proposed implementation starts with the user generation section. On user generation, the user can create an account by either creating a new account or by using Google, Facebook, or LinkedIn details. Next, the user is allowed to select three images randomly from a board with numbers. This image selection is done at random, along with random pin generation, in the format of 4-6-8 and it will not change once selected. The user must be alert when providing the same authentication images whenever logging in. The main reason for random selection is that there is a possibility of one or more users selecting the same authentication image, which leads to severe damage. The random selection has a

unique key that will only work for one user and it will not repeat for any other user using the cloud. If means successfully an account is created for the user, the user can log in by providing authentication images and a pin if they match the user logged in, otherwise rejected.

The authenticated user can then use the cloud database. The user can select any big data files from its formats as per their choice of requirements. Once the file is selected, it undergoes the implementation of the RSA algorithm. Here, two stages of the process are completed, namely, the creation of public and private keys, followed by file encryption and storage in the cloud database. Then the user can be logged out and the same manner is followed for viewing the original file that is undergoing decryption by providing the private key. The working mechanism of RSA is discussed in detail in the next section. Below is the step-by-step process of the proposed ERSA implementation.

Step-1

User registration process

Enter the name and personal details;

Select the random images (3 or 4,6) as per user choice;

Generate the random pin;

Step-2

User validation process

User pin & images are correct(match);

Account will activate;

Otherwise;

Reactivate; // same process repeat; step-1

Activation complete

File and data types

File type (doc, pdf, xls,.dat,.jpeg,.png,.avi)

}

Otherwise

Login (google, fb, linked based on login)

End if;

End.

3.2 Working of RSA Algorithm

RSA is an asymmetric cryptography algorithm that has both a public key and a private key. The two keys come along with the security key. In this methodology, the original text and ciphertext are the integer between 0 and n-1. For RSA the n size 1024 bits RSA is a cipher in a block where all messages are integers. The two keys generated are a public key and a private key where the public key is visible to all. But the private is known only by the data owner. Based on that key only the data owner can decrypt the file to get the original information. RSA involves three steps such as;

- Key Generation
- Encryption
- Decryption

Key Generation: The key generation is done directly between the user and the cloud provider which must be done before the file encryption. The key generation algorithm is expressed as below;

Step 1: Two distinct prime number is chosen such as p and q. These should be integers chosen randomly with a similar bit length.

Step 2: Calculating n = p * q

Step 3: Calculating Euler's totient function

$\varnothing(n) = (p-1) * (q-1)$

Step 4: The integer f is taken, such as $1 < f < \varnothing$ (n) and the greatest common divisor of f. $\varnothing(n)$ is 1 where the f is the Public-Key exponent

Step 5: Applying g, a Private-Key exponent $g = f^{-1}(mod \varnothing(n))$, so g * f = 1 mod$\varnothing(n)$

Step 6: Apply fuzzy set to private key

Step 7: The public-Key modulus f i.e (f, n) and private–key modulus g i.e., (g, n)

Encryption Algorithm

Encryption is the process of converting the plain text into ciphertext, which can be done by the following steps;

Step 1: The cloud service provider share the generated public key (f, n) to the user for data storing

Step 2: The data is mapped to an integer according to reversible protocol referred to as padding scheme.

Step 3: Data is encrypted into a ciphertext C, $C = m^f (mod\ n)$ and the encrypted data is stored in the cloud database

Decryption Algorithm

Decryption is the process of converting the ciphertext into the original text by employing the authentication key.

Step 1: The user requesting the cloud provider for the data

Step 2: The authentication verification is done if successful the file (cryptic data) C is given

Step 3: Decryption process, $m = C^g (mod\ n)$, Once m is obtained the original file is viewed through reversing the padding scheme.

3.3 Fuzzy Set to Private Key

The process of applying a fuzzy set to a private key is described in this section. The fuzzy logic is similar to human interpretation and it frames the intermediate possibilities as digital values between 0 and 1. The Boolean postulates for Yes or No are considered for this fuzzy logic so that the conditions can be obtained as Yes, Near Yes, Ideal, Near No, and No. The steps followed in the general fuzzy logic start from defining the variables. Here the variables represent the public and private keys. For the variables, a fuzzy set is generated using the fuzzy membership function. The results obtained in the fuzzification process are combined in the inference engine and finally, the data is converted into non-fuzzy values which are the last step of defuzzification in the fuzzy logic. To define the fuzzy set we consider the members as positive, near positive, Neutral, near negative, and Negative. Consider, for instance, the public key is generated as 56 then the fuzzy set will be generated as

$Key\ (i) = 55.8,\ 55.9,\ 55,\ 55.1,\ 55.2$

The membership functions for the given variables are generated in the inference engine using fuzzy IF-THEN rules. The logical operators used in this process are AND, OR NOT along with MAX and MIN functions. The MIN function is used for AND logic and MAX function is used for OR logic and the Complement function (1-X) is used for NOT. The logic table for the functions is similar to its basic logic which is depicted in Tables 1–3.

Table 1: $MIN\ (P,\ Q)$ resolves set $P\ AND\ Q$

P	Q	$P\ AND\ Q$	$MIN\ (P,\ Q)$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Table 2: $MAX\ (P,\ Q)$ resolves set $P\ OR\ Q$

P	Q	$P\ AND\ Q$	$MAX\ (P,\ Q)$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Table 3: $NOT\ P$ equivalent for $1 - P$ (Complement)

P	NOT P	$1 - P$
0	1	1
1	0	0

The fuzzy variable functions for the cryptography process in the inference engine for the variables given in Tables 1–3 are defined as follows.

$MIN\ (TRUTH(X),\ TRUTH(Y)) \rightarrow X\ AND\ Y$

$MAX\ (TRUTH(X),\ TRUTH(Y)) \rightarrow X\ OR\ Y$

$(1 - Truth(X)) \rightarrow Not\ X$

Based on the fuzzy IF-THEN rules a rule base is created and the sample rule is illustrated as follows.

$$"IF\ Key\ =\ (A_2\ OR\ A_1)AND\ NEUTRAL = AB\ THEN\ IF\ Key =\ (B_1\ OR\ B_2)AND\ NEUTRAL$$
$$= AB\ THEN\ IF\ Key = AB\ AND\ NEUTRAL = AB"$$

A fuzzy matrix is obtained for the input variables in the fuzzy inference engine and it is depicted in Tables 4.

Table 4: Inference engine fuzzy matrix

Key	A_1	A_2	AB	B_1	B_2
A_1	No change	Add	Add	Add	Add
A_2	Subtract	No change	Add	Add	Add
AB	Subtract	Subtract	No change	Add	Add
B_1	Subtract	Subtract	Subtract	No change	Add
B_2	Subtract	Subtract	Subtract	Subtract	No change

The results obtained from the fuzzy inference engine are combined to obtain the final results. The operators and functions are involved in the final process so that the fuzzy values are obtained. The obtained values are converted into non-fuzzy values in the defuzzification process based on the membership function.

4 Proposed Methodology Work Flow

Fig. 2 the user creates a cloud account to use the cloud database. There are two methods: by creating a new account or by providing their existing Google, Facebook, or linked account details. In this first level of the authentication scheme, choose the image and PIN randomly. Once this stage is completed, the user registration process is complete. The chosen authentication is needed to provide for further processing. If the user logs a request by providing the image and pin, if it is valid, the user could use the cloud database. At this stage, second-level security key generation occurs between the user and the cloud service provider. The user is allowed to choose a file of the own type to be stored in the cloud. Before storing it, it is encrypted using RSA by choosing the largest prime number. A public key is generated and a fuzzy set is applied before the encryption process which is visible to both the user and the cloud provider. Based on that key, only the user can store the encrypted file in the cloud. In the same manner, the public key-only cloud provider responds to the user with the appropriate file. The private key is only known to the data owner, who can use it to decrypt the file and retrieve the original data.

5 Experimental Result

The experiment is conducted between our proposed ERSA with DSSE and EFSSA for performance evaluation Fig. 3. The observation is based on the three functions such as key generation, encryption process, and decryption process. All work is done on Intel(R) Core-2 with CPU 1.4 GHz processor, 4 GB RAM on Windows7 or more working framework by using MATLAB. The file size used for encryption is from 256 Mb to 2.5 GB and the respective key sizes will be from 256 MB to 2.5 GB. In the performance analysis, time consumption plays a vital role, algorithms efficiency is declared by the time taken for a certain process. By varying the file size the encryption and decryption time is measured with different key sizes from 256 MB to 2.5 GB and based on the computation time, throughput for the encryption and decryption process is observed for performance analysis. The design of an optimized system results in minimum time consumption on the cryptography process. Let's see the comparative analysis of these three algorithms;

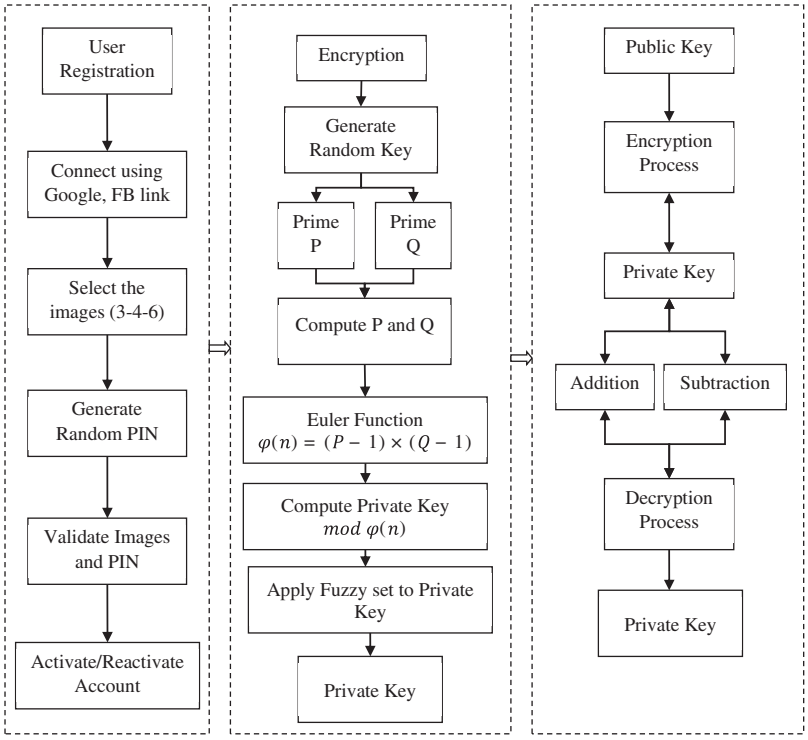

Figure 2: Proposed workflow

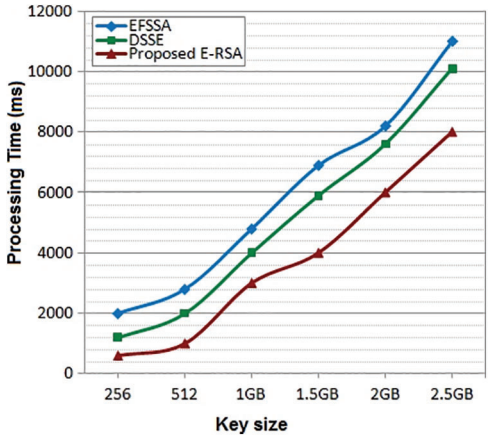

Figure 3: Key generation process *vs*. time consumption between three algorithms

The key generation is processed between the cloud service provider and the user based on the privacy policy. Fig. 4 shows the key generation done with the different workloads and computed with the algorithms. Simultaneously the processing time taken by each algorithm is noted and plotted on the graph. It shows that the processing time of our proposed ERSA is less, as compared to the other two algorithms DSSE and EFSSA. In a key generation, our proposed ERSA is more effective with minimum time consumption.

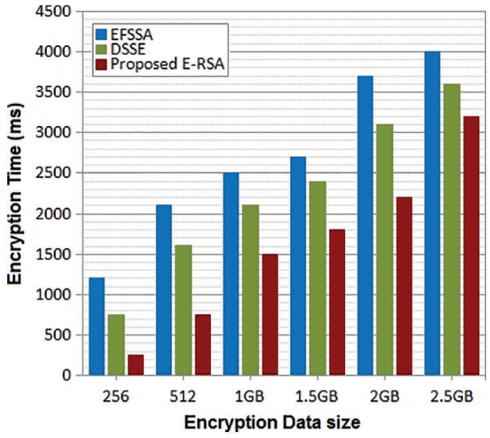

Figure 4: Encryption process *vs*. time consumption between three algorithms

Encryption is the process of converting plain text into ciphertext. Our proposed ERSA uses 1024 bits for encryptions. The above Fig. 5 is the comparative results between these three algorithms with various workloads. The time consumption taken by three algorithms is noted and based on the results on the graph. The performance of ERSA is more effective than the DSSE and EFSSA respectively. It shows that the time taken by ERSA is very less compared to DSSE and EFSSA.

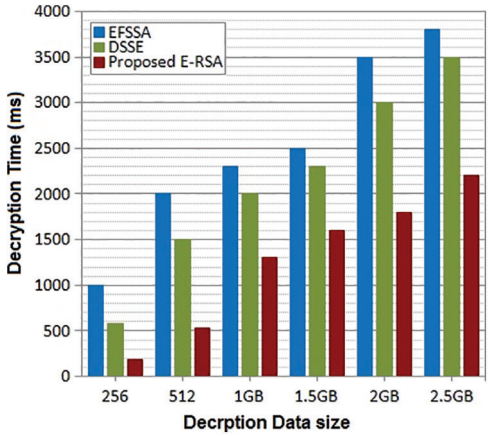

Figure 5: Decryption process *vs*. time consumption between three algorithms

Decryption is the process of retaining the original text by providing the original key. In this process, these three algorithms are applied for decryption as per various workloads, which are the same as taken for encryption. The time consumed by three algorithms is noted and plotted in the graph. Fig. 6 is the observation of the decryption process among the three algorithms. The time consumed by ERSA is very minimal compared to DSSE and EFSSA. Thus our proposed method is efficient in the decryption process. On the above three observations, it is proved that our ERSA is prominent with minimum time consumption and increases the security level with an image along with a pin mechanism.

Figs. 6 and 7 depict the encryption and decryption throughput for the proposed and existing algorithms. The encryption throughput is obtained as an average value as a ratio of total text encrypted to encryption time. Similarly, the decryption throughput is obtained as a ratio of the average total cipher text to the decryption time. It is observed from the results, that the maximum throughput is attained by the proposed

enhanced fuzzy-based RSA scheme whereas the existing models exhibit less encryption and decryption throughput. The maximum throughput attained by the proposed E-RSA is 500 Mb/Min whereas DSSE attains 350 Mb/Min and EFSSA attains 310 Mb/Min which is much lesser than the proposed model encryption throughput. In the case of decryption throughput, the maximum value attained by the proposed E-RSA is 480 Mb/Min whereas DSSE attains 330 Mb/Min and EFSSA attains 290 Mb/Min which is much lesser than the proposed model decryption throughput. From the results, it is observed that the proposed encryption procedure will be a suitable big data environment to secure the user data compared to existing encryption algorithms.

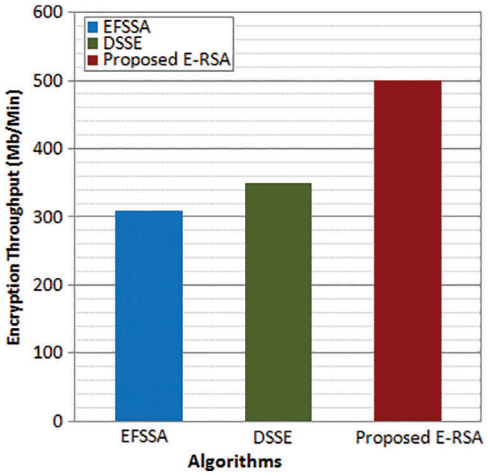

Figure 6: Encryption throughput

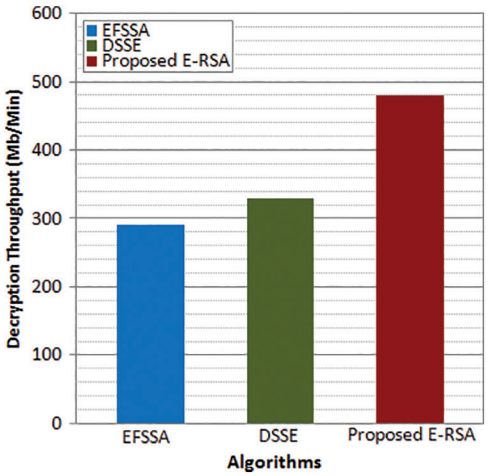

Figure 7: Decryption throughput

6 Conclusion

In big data, flexibility and reliability are well praised by the users. The major user concern in the cloud system is security issues, as they store their highly sensitive data in the cloud database. To this, several works are evolved with the cryptography mechanism among which the known algorithm is RSA. RSA is an asymmetric algorithm that uses 1024 bits. It is considered a highly secure mechanism that prevents intruders and data leakages. We found that the security level during authentication needs to be improved

which makes RSA more enhanced. In this way, we proposed an E-RSA with random image selection and pin generation schemes. This ensures the authentication level in a greater manner by which only an authenticated user will be logged to a cloud account. Then the user can utilize a cloud database for file uploading or downloading and stored securely with encryption using RSA. The proposed work security level is compared with existing DSSE and EFSSA. The observation is carried out on three metrics such as key generation, encryption, and decryptions. The obtained results are plotted on the graph and their performance levels are discussed based on time consumption with various workloads. The observation shows ERSA shows a fair improvement level on comparing with others, thus ensuring the user privacy in a qualified standard.

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] S. K. Ocansey, W. Ametepe, X. W. Li and C. Wang, "Dynamic searchable encryption with privacy protection for cloud computing," *International Journal of Communication Systems*, vol. 31, no. 1, pp. 3403, 2018.

[2] K. V. Pradeep, V. Vijayakumar and V. Subramaniyaswamy, "An efficient framework for sharing a file in a secure manner using asymmetric key distribution management in cloud environment," *Journal of Computer Networks and Communications*, vol. 2019, no. 9852472, pp. 1–8, 2019.

[3] B. B. Gupta, S. Yamaguchi and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 9203–9208, 2018.

[4] P. Jain, M. Gyanchandani and N. Khare, "Enhanced secured map reduce layer for big data privacy and security," *Journal of Big Data*, vol. 6, no. 1, pp. 1–17, 2019.

[5] S. Alouneh, F. Al-Hawari, I. Hababeh and G. Ghinea, "An effective classification approach for big data security based on GMPLS/MPLS networks," *Security and Communication Networks*, vol. 2018, no. 8028960, pp. 1–10, 2018.

[6] R. Mudgal and M. K. Bhatia, "International journal of engineering sciences & research technology enhancing data security using encryption and splitting technique over multi-cloud environment," *Engineering Science Research Technology*, vol. 7, no. 8, pp. 440–449, 2018.

[7] S. Belguith, N. Kaaniche and M. Hammoudeh, "Analysis of attribute-based cryptographic techniques and their application to protect cloud services," *Journal of Computer Networks and Communications*, vol. 2019, no. 3667, pp. 1–19, 2019.

[8] N. Kaaniche, S. Belguith, M. Laurent, A. Jemai and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," *Computer Networks*, vol. 133, no. 7, pp. 141–156, 2018.

[9] H. Xiong, Y. Zhao, L. Peng, H. Zhang and K. H. Yeh, "Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing," *Future Generation Computer Systems*, vol. 97, no. 5, pp. 453–461, 2019.

[10] H. Zhong, W. Zhu, Y. Xu and J. Cui, "Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage," *Soft Computing*, vol. 22, no. 1, pp. 243–251, 2018.

[11] F. Zhao, T. Nishide and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *Proc. of 7th Int. Conf. ISPEC*, Guangzhou, China, pp. 83–97, 2011.

[12] A. Ge, C. Chen, C. Ma and Z. Zhang, "Short and efficient expressive attribute-based signature in the standard model," *Cryptology ePrint Archive*, 2012.

[13] Z. Liu, H. Yan and Z. Li, "Server-aided anonymous attribute-based authentication in cloud computing," *Future Generation Computer Systems*, vol. 52, no. 9, pp. 61–66, 2015.

[14] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hop-byhop authentication scheme for filtering of injected false data in sensor networks," in *Proc. of IEEE Symp. on Security and Privacy*, Berkeley, CA, USA, pp. 259–271, 2003.