Securing of Cloud Storage Data Using Hybrid AES-ECC Cryptographic Approach

Sunil Kumar* and Dilip Kumar

Dept. of Computer Science & Engineering, National Institute of Technology, Jamshedpur, India
E-mail: 2018rscs016@nitjsr.ac.in; dilip.cse@nitjsr.ac.in
**Corresponding Author*

Received 27 February 2022; Accepted 22 June 2022;
Publication 15 November 2022

Abstract

Internet has revolutionized the world in a way no one could have ever imagined. It paved the way for various different technologies, that have transformed the world exceptionally. Internet enabled cloud technology which provides cost-effective, scalable, on-demand computing resources with little to no downtime. Cloud storage allows its users to store and access private data from anywhere in the world without needing any high-end computing system. Cloud storage isn't always secure, but that doesn't imply it isn't. The security of a data depends on the security policies followed by the provider along with the security of the communication channel via which the data is being sent. Encryption is used to obfuscate the data so that it can only be viewed when correct credentials, known as encryption keys, are provided. Following study proposes an encryption technique using ECC (Elliptic Curve Cryptography) along with AES (Advance Encryption Standard) to provide data confidentiality in an efficient way for securing data on cloud and hence, protect the personal information of user from any adversary. This new method is more effective, and the results are superior as a consequence.

Keywords: Symmetric encryption, asymmetric encryption, ECC, AES, blowfish, cloud storage security and authentication.

Journal of Mobile Multimedia, Vol. 19_2, 363–388.
doi: 10.13052/jmm1550-4646.1921

1 Introduction

Cloud computing provides an on-demand delivery of various kinds of services via the Internet. It allows us to access and maintain the hardware as well as software resource that we own remotely i.e., the resource can be controlled from anywhere in the world and from almost every available platform. It increases resource sharing and organizations of various sizes can host their websites and application on cloud servers of third-party service provider without worrying about all of the internal workings. Depending on the organization's needs, they can choose from various types of services that exists over the cloud. Among various computing models, Cloud Services is one that provides a wide range of services regardless of location or media, and is easily accessed from any location. Its appealing features have increased reliance on the cloud, resulting in large data volumes and privacy and security problems. Cloud users may cause significant disadvantages, such as data security and data leak, either purposefully or unintentionally. Unauthenticated and unauthorized sources should be restricted from data access. Devices can also leak data if users are allowed to reuse APIs and data.

Cryptography, steganography, hashing and other methods can be used to protect data. For hundreds of years, conventional methods like message encryption have been used to make confidential communications virtually unintelligible. Encryption systems based on AES, and ECC can be used to secure cloud storage data, such as images, textual files, audio files, and videos [1].

Using keys, two types of encryption techniques can be employed to secure data.

- Encryption of data using Asymmetric key and
- Encryption of data using Symmetric key.

Public-key cryptography, or asymmetric key encryption, is another name for it. In order to decrypt and encrypt the message, it contains a pair of private and public keys, which are used in tandem. In addition, symmetric key encryption, where data are encrypted using a single private key and subsequently decrypted, is also used to protect data. In order to keep the message safe from hackers, the private key is used. The challenge in adopting symmetric cryptographic techniques originates from the size of the key, which must be large enough to provide sufficient security.

Even in the presence of an attacker, cryptography can be used to communicate safely. As a general rule, the sender encrypts his or her message before sending it over the communication channel. The receiver, by some means, is

able to convert the cryptic data back into the original message. Cryptographic techniques have been used for well over centuries. "Caesar Cipher" was used by Julius Caesar to communicate with his generals. Essentially, each character of the message was shifted by a fixed number of spaces to yield a new alphabet [2]. There could be only 25 other possible shifts of any ciphered English alphabet, it will take an only fraction of seconds to break the cipher. Encryption can be either symmetric or asymmetric. In symmetric, we use the same key for both encryption and decryption. But in asymmetric one key is used to encrypt the data, while the other is used to decrypt it. Symmetric encryptions/decryptions are usually faster but the shared secret keys must be known to both communicating parties in advance. So, there is a problem with sharing the secret key.

To increase system security, Chen et al. [6] recommended using AES with ECC, which they argued would be more secure. Although there are numerous techniques of authentication, there is no reduction in computing time or cost. On the other hand, asymmetric allows the sender to make one of their key publics and keep the other private. Anyone can encrypt the data with the sender's public key and the only sender will be able to decrypt it with the corresponding private key. The asymmetric key-based algorithm usually lacks in time efficiency, however. Here, a hybrid encryption technique is used where both symmetric as well as asymmetric encryption algorithms are used. The system is capable of encrypting any type of multimedia data (Text, images, etc.) and provides the same (or even) better security while remaining time and space-efficient.

The paper describes a hybrid approach for securing the data over the cloud. The proposed technique uses a combination of a symmetric encryption (AES) and an asymmetric encryption (ECC) algorithm to encrypt and decrypt the data. The data is first encrypted with AES using the key generated by Elliptic curve algorithm. The encrypted data is then encrypted with ECC public key. During decryption, the data is decrypted firstly with ECC private key of the receiver and then with AES.

The paper proposes another way of using hybrid technique to encrypt and decrypt data that is to be communicated over the cloud. The symmetric algorithm used for encryption is AES. It will be used for encrypting the data which is to be communicated. The proposed algorithm also uses ECC. The secret AES key is encrypted with the public ECC key of the receiver. Both the encrypted AES key and the encrypted data is sent over to the receiver or to the cloud. When decryption, the encrypted secret key is decrypted using the ECC private key, which will then be used to decrypt the ciphered data

1.1 Characteristics of Cloud Computing

Data can be securely transmitted from various locations to a "cloud" server, which can then be accessed from any location at any time using any device. Cloud computing has a variety of properties that allow it to give services to a wide range of customers, regardless of their type of work. Characteristics like [8] are to be expected.

Various cloud storage developments have made it possible for consumers to have their data encrypted and decrypted without the participation of a third party. Increased security and storage efficiency for secure access and rapid data retrieval are achieved by this enhancement. Incorporating cryptographic approaches, this service makes it simple for diverse sorts of users to shared cloud resources, while also enhancing the system's overall capability [8].

1.1.1. ***Network Access*:** Every user will have no problem accessing their data from any location or on any system because the network is widely available to everyone.

1.1.2. ***Expeditious Elasticity*:** The interface is simple to use and can be customized According to their needs, customers can store data on the cloud using this service.

1.1.3. ***On-Demand Self-Service*:** Due to the fact that many self-services are provided without the authorization of the service provider, cloud computing promotes the supply of such services.

1.1.4. ***Shared Resources*:** The allocation and distribution of resources is based on the unique needs of each individual user.

Figure 1 Serves of cloud computing.

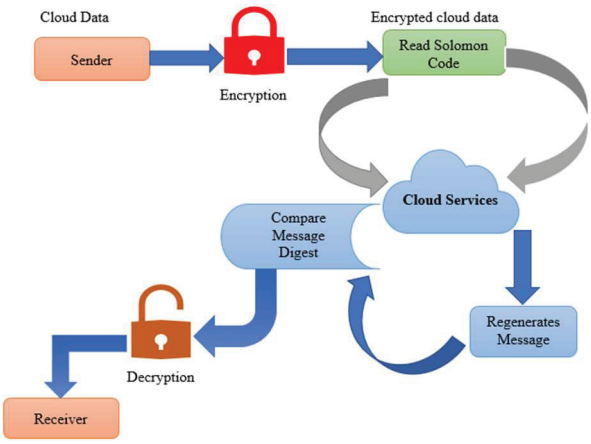


Figure 2 Cloud computing-based service.

1.1.5. ***Measured and Managed Services*:** The service providers are in control of things like data organization and cloud storage security management for each individual user. Figure 1 depicts the primary cloud computing services.

1.2 Cloud-based Cryptography Services

Cloud storage developments also made it possible for consumers to have their data encrypted and decrypted without the participation of a third party. Increased security and storage efficiency for secure access and rapid data retrieval are achieved by this enhancement. This service makes it easy for different sorts of customers to share cloud resources and increase the system's capacity by implementing cryptographic procedures [9]. The cloud server can be observed encrypting and decrypting the data sent and received between the sender and recipient. In Figure 2 shows the cloud storage services that are available in different types. Secure data transmission is also an important aspect of storage service of cloud.

1.3 ECC (Elliptic Curve Cryptography)

It's possible to get cloud service that is very good in the form of ECC, which is used to protect data to ensure the security of your data, you can employ ECC, a cloud service that provides excellent protection. These services encrypt and

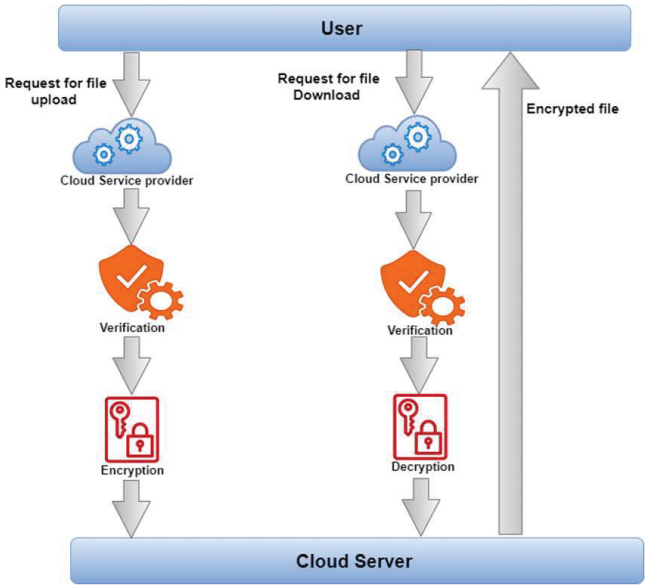


Figure 3 Cloud storage server.

decrypt your data using asymmetric encryption and decryption. The use of RSA to encrypt and decrypt data makes it faster than other methods.

To make things even better, this method of symmetric encryption and decryption has a smaller key size than the other one. RSA is used in ECC as an illustration of how it works. The RSA algorithm will reduce the key size to 163 bits if it is 1020 bits long. ECC is also more suitable for those who access the internet mostly through their mobile phones. To avenge themselves, they're looking for the user's personal information or other data. As a result, ECC was designed for those who need to access their data from a vulnerable device [10]. Figure 3 demonstrates how a user's data request is processed by the server and how the data can be obtained in a secure manner.

1.4 Contribution

The main contributions of this paper are listed here.

1.4.1. With the use of ECC, we offer a hybrid approach in which the AES key is generated using the ECC algorithm. Essentially, this means that we are not employing an AES key generation method; rather, we are employing the ECC approach to generate our key.

1.4.2. Information is encrypted and decrypted using a public key or a private key, much like in symmetric or asymmetric encryption. Big key size is needed, as well as a lot of computer capacity, for this operation. With the suggested hybrid technique (AES-ECC), the problem of key size can be solved quickly while also lowering computing requirements for storage minimization.
1.4.3. The ECC technique is used to generate a public key, while AES is used for encryption and decryption in our new framework.

1.5 Organization of the Paper

Apart from the introduction, related work is done in Section 2. Existing cryptography algorithms are described in Section 3. The proposed hybrid approach is shown in Section 4. Results and implementation are done in Section 5. and, the conclusion is in 6.

2 Related Work

There are a lot of different scholars and researchers who have written about data security and math in this literature review. The main focus is on the following literary works. The following papers have been chosen for review in light of the traditional and traditional approaches to cryptography, as well as newer techniques. It is used in this paper to make a text-based Elliptic Curve Cryptosystem work. A value for each character in a message is shown by its ASCII code number. This is how each of these ASCII values is turned into an affine point on the EC. The starting point is called Pm. As part of this study, plaintext ASCII values can be transformed by utilizing an affine point. There are two reasons for this change. The ASCII integer of the character is first transformed into a set of coordinates that fit the EC. Second, by introducing non-linearity, the character's identity is completely obscured. The ECC method is used to encrypt the message's converted character [2].

AES and ECC are suggested in Ref. [3] as ways to improve system security. In order to distribute and manage the system without a trusted center, Shamir secret sharing is used. There are still significant computational and time expenses associated with implementing the proposed combination method, even though it boosts system security [4]. Furthermore, the service provider ensures that data is quickly accessible and managed effectively. The influence of plain text and data block size on cloud computing data services is also measured.

When 256 bits of data match NIST criteria, the security of ECC and RSA can be coupled by employing data exceeding 264 bits in the study [5] by Madhavi et al. Because the ECC provides a more secure service across smaller amounts of data and has less storage space for data access, it is more effective than the RSA algorithm in this regard. Different JAVA platforms allow for experimentation. A variety of customers can benefit from ECC's encryption and decryption capabilities [6, 7, 9].

The layered approach, which consists of two portions for encryption and decryption, is used. Small parts in the first section are used to add additional bits to the data encryption process and to minimize the key size for easy accessibility. A partition of elliptical curves like P0, P1, P2, P3, P4, and so on make up the second layer; these are used to encrypt data. These steps are used to encrypt and decrypt the data, and these two levels offer the data's security. There are security and data loss risks in the preceding methods. In order to deal with these issues, ECC is employed to protect data and keep it safe from unauthorized access. Using this asymmetric method of cryptography, massive datasets may be easily protected and enhanced so that security services can be provided the most quickly. Data can be accessed and protected via cloud computing at the same time via ECC.

In the publication [10], hybrid methods for RSS and ECC are employed. After the data have been reduced, the elliptical curve authorities are given some signature components to sign and digest the message. ECC may use encrypted data for this purpose from time to time. There is no difference between the encryption and the encryption process.

Multiple methods are used to protect data encryption and decryption during transmission. That report mentions the integrity and confidentiality of the data. Data authentication is critical in various new devices, such as Internet of Things (IoT) devices. Authentication is critical for these devices because of the large amounts of sensitive data that are stored there. The device's cryptographic activities necessitate a powerful processor. These devices rely on clouds to authenticate data and carry out protocol execution.

For cloud computing data security, papers [11] were prepared with the use of a two-level cryptographic technique and a new idea. As a result, intruders can't get their hands-on real information, which improves privacy, the value of information, and the time it takes to do cryptographic tasks. A system's invaders need to be kept at arm's length from the highly sensitive data being transmitted. Cryptography utilizing Elliptic Curve Architectures is a relatively new branch of network security that relies on elliptic curve arithmetic and discrete logarithmic issues. Encryption, digital signatures, and

key exchange are all made possible using ECC systems, which use public-key cryptography. Security capabilities like secure email, safe Web browsing, and virtual private networking to corporate networks are becoming increasingly important for wireless devices, and ECC makes it easier to implement all of these functions [12]

In terms of security and efficiency, ECC is superior to the first-generation public-key approaches that were used. Researchers in this work are hoping to evolve both AES and Blowfish into low-power, high-throughput cryptographic algorithms that are dependable and exceptionally safe at the same time. The estimation of both algorithms seems unattainable. Symmetric ciphers like AES, DES, and blowfish are compared to the asymmetric cipher RSA in the hybrid encryption system under examination. Among the four ciphers examined in the study, RSA is the most secure, utilizing keys with a minimum of 1024 bits of length [15, 16].

For cloud computing services, security and privacy protection are critical issues. Because the CSP is an outsider, we are unable to keep raw information without encrypting it because of security concerns. Using a cross-breed cryptosystem, the authors of the proposed paper discuss how to provide reliable cloud-based information transmission and storage. Cloud information can be more secure because to the use of both symmetric and divergent encryption, which can be implemented simultaneously to strengthen the framework's trustworthiness. As a result, the predicted model manages a more secured and efficient AES and ECC-based encryption technique [18, 19].

Using cryptography to secure distributed storage was discussed in papers [20, 21]. AES, ECC, and RSA were among the standard cryptographic tools used to achieve this goal of privacy preservation. Finding an efficient and secure encryption system was addressed by these studies, despite their disparities in presentation. When it comes to encoding and decrypting data, even while some systems offer high levels of security, the procedure can be time-consuming. The demand for security impedes the effectiveness of different encryption algorithms in the other direction.

In reference [22, 23] presented a two-level cryptographic technique in order to improve data security in cloud computing. Cryptographic algorithms such as AES and ECC are used to increase the security of data against intruders, keeping them from accessing the genuine data, increasing privacy and integrity of data, and reducing the time required to execute cryptographic activities.

Detailed comparative comparison of related work is presented by Table 1.

Table 1 Comparative analysis of related work

Reference	Tool Used	Technique Used	Limitation
3	JAVA in Eclipse	AES-ECC along with Shamir secret key	The CSP does not contain any information regarding a user's private key or the public key of that user.
7	iFogSim	Point Multiplication in Hybrid approach	Cloud computing has lower levels of data security.
8	PYTHON	Irondale encryption algorithm with EAP-CHAP	EAP-CHAP necessitates a significant amount of processing power.
24	JAVA	Cryptography based on polynomial-based elliptical curve hashing	Because the hash values must be encrypted as well, PHECC enlarges the size of the secure messages.
25	JAVA in Netbeans	experimental time evaluation and Hybrid algorithm	Because cloud storage's user verification process is so slow, a large number of users must use alternate methods to complete their registrations.
26	AESCrypt and OpenSSL in the Kali Linux	AESCrypt Two-layered approach	Only a few fields are available for ECC operations.
27	Verilog Programming Language	8-bit Elliptic Curve Crypto-processor	Because the Karatsuba multiplier doesn't have bi-linear pairing, ECC-based lightweight devices are less secure than if they had ECC. Decryption can't go on, and it doesn't have as much room to grow.
28	Python	Holistic Security Model (AES 256-bit)	Users' data can be snooped on during the process of moving it from the user's computer to the cloud. People who try to break into someone else's data through cloud segmentation can do so.

2.1 Problem Statement

There are some problems with existing technologies that need to be taken into account when developing new encryption models for multimedia data. There is a need for better encryption models for multimedia data in terms of both security and time. A new system has been proposed to address these issues and these other needs [22].

2.1.1. ***Key Size*:** Because symmetric cyphers require only a single key for both encryption and decryption, they are considered to be more secure, the key must be extremely large to prevent brute force attacks from guessing it. For better security and less memory usage, asymmetric ciphers use two keys to accomplish the same thing.

2.1.2. ***Time Complexity*:** Design approaches that require a lot of time to implement are more complicated, whereas those that require less time but sacrifice security are simpler. As a result, a compromise must be made between the two.

2.1.3. ***Memory-Efficiency*:** It's a trade-off: Text encryption is more memory efficient than multimedia file encryption, but it doesn't have as much diversity. Multimedia file encryption takes more free memory space because it needs to store the encrypted files and the keys. A compromise between diversity and memory must therefore be made once more.

2.1.4. ***Types of Inputs supported*:** Only single-functioned encryption was found in all of the literature evaluated Encryption of text inputs didn't work well when it came to high-requirement multimedia inputs like images and audio and video, as well as graphical content and so on [22]. The amount of memory it takes to encrypt and decrypt, as well as the amount of time it takes to do so.

3 Earlier Used Cryptography Algorithms

Advanced Encryption Standard (AES), Blowfish, and Elliptic Curve Cryptography are used in the proposed methodology they are explained:

3.1 Advance Encryption Standard (AES)

In substitute of the current Data Encryption Standard, the Advanced Encryption Standard was proposed (DES). As an input, it accepts a 128-bit plaintext

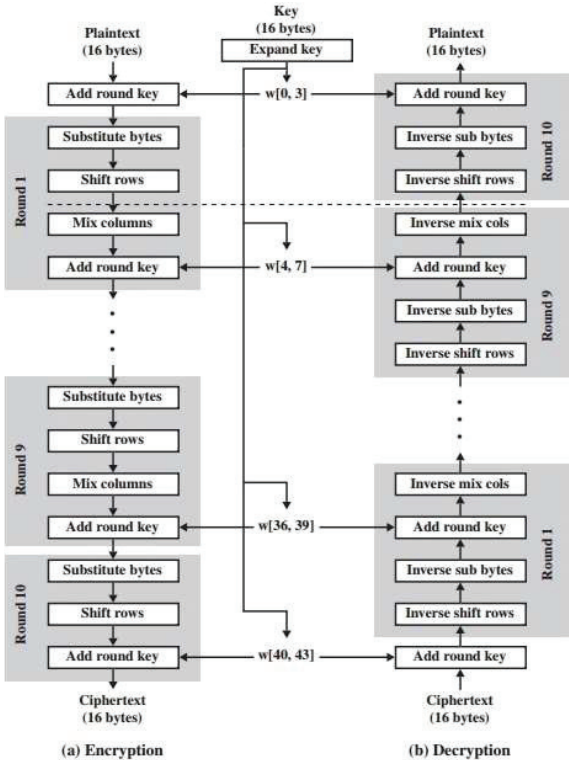


Figure 4 Working of AES encryption and decryption.

and encodes it with one of the following keys: 128/192/128/256-bit or 10/14/128/192/128/256.

In contrast to the Feistel encryption used in the DES algorithm, AES does not use the Feistel cipher. For encryption and decryption using AES, see Figure 4. for a breakdown of the many internal rounds. Bit-by-bit replacement, row shifting (transposition), column mixing, and adding round keys till n-1 rounds are the main components. The last nth round does not include a mixed column round. A 128-bit ciphertext is generated after the nth round.

3.2 Elliptic Curve Cryptography (E.C.C)

Neal Koblitz along with Victor Miller discovered the ECC in 1985. An elliptic curve, with two variables, over a field K, is non-singular cubic curve such that

$$f(x, y) = 01$$

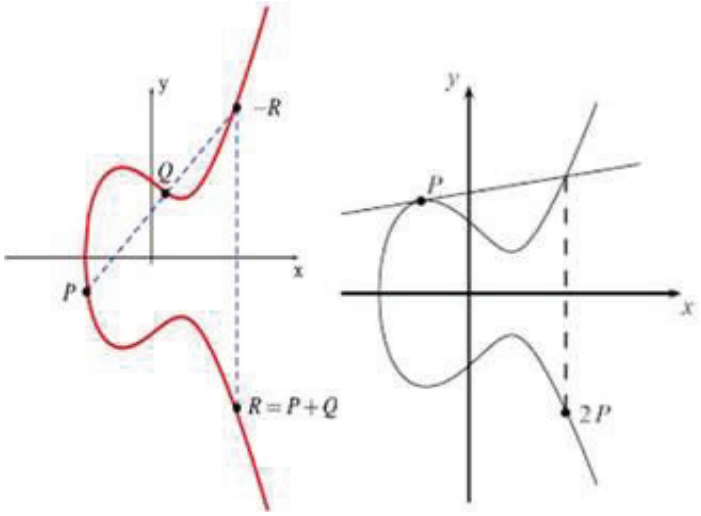


Figure 5 (a) Point addition. (b) Point Doubling.

An elliptic curve is defined by an equation of the form:

$$y^2 = x^3 + ax + b2$$

Using point doubling as well as point addition any point P (x, y) on the elliptic curve can yield the resultant point P' (x', y').

Figure 5(a) and 5(b) shows the elliptic curve addition in which, a straight line is formed by joining the two points that are to be added. The negative equivalent of the point at which the straight line intercepts the curve is taken which is the final result. For point doubling, simply the tangent of the point is allowed to fall on the curve, and the negative equivalent of the point where the tangent intercepts the curve is the result. The great advantage of ECC is that even a smaller key is stronger than a comparatively larger RSA key. The strength is based on the fact that solving the discrete logarithmic problem on an elliptic curve with respect to a publicly known base point is a hard problem. The public key of the ECC is the base point on the curve while the private key is just an integer describing the number of dots. The keys in the ECC system are not interchangeable. The security and speed lie in the fact that it is very easy to compute a final point if the base point and the number of dots that occur are known. However, given the base point and the endpoint, it is very hard to compute the number of dots that were taken to get there [13, 14, 17].

4 Methodology and Proposed Hybrid Approach

4.1 Research Methodology

Here, we present a brief description of the research methodology used in the work. In the following section, we'll go through the proposed method's research strategy in more detail. We can observe from Figure 6 that the manuscript follows the typical research flow. Initially, we looked at the literature to see what other people had done. We discovered a number of flaws in the current methods after doing extensive research. We discovered that present techniques have higher computation overhead costs and longer computation times. However, our novel hybrid solution (AES-ECC), which secures data via the cloud, addresses only a few of the key drawbacks. Our proposed hybrid scheme is tested and compared to other approaches and other hybrid schemes, as well. We discovered that our hybrid security system improved and outperformed other security systems.

4.2 Proposed Hybrid Approach

Data security is a big problem right now, and it can be harmed in a number of ways, both from outside and inside the company. When data is sent over the Internet, different encryption methods are used to make sure it doesn't get stolen. People don't like how these techniques work because they need a lot of keys, memory space and computer power to secure the information

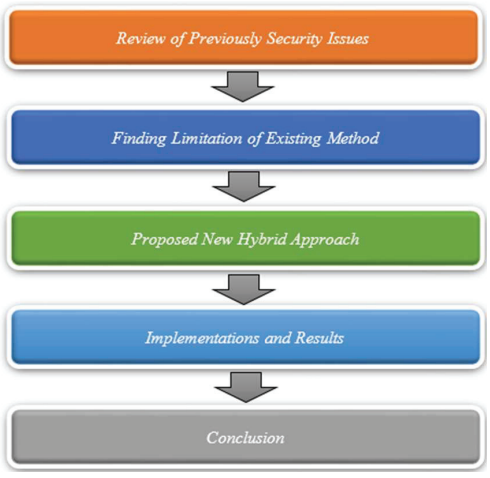


Figure 6 Research methodology.

from being stolen after uploading an input file, an AES-encryption-style key is generated.

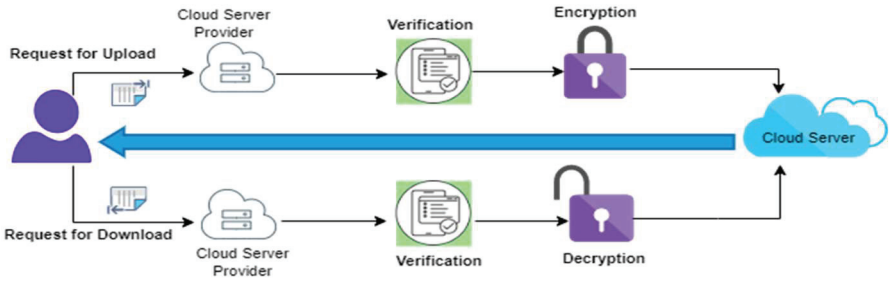
In other words, because AES is symmetric in nature, only one key is required for both encrypting and decrypting data. The third party should be able to figure out how to decrypt and encrypt the input file because only one key is required. As a result, the user will be completely unaware that their input file has been accessed by a third party. One of the most secure algorithms in existence, AES is vulnerable if the sole key is known. The public and private keys are used for encryption and decryption. An asymmetric encryption system like ECC employs two keys for encryption and decryption. Thus, its security is enhanced, and it is difficult to break both keys simultaneously. Additionally, ECC's low-key size is well-known. ECC can be as secure as other approaches even with a smaller key. Need to make an encryption and decryption system that costs less and takes less time to make.

This way, the data over the cloud will be safe. We combine the good things about both algorithms and use them in our new model. In the Figure 7 below, it can be seen that AES and ECC work well together to keep data safe when it is stored on the cloud. The new diagram shows that the new method is very different from the old one. In this diagram, the user's data is sent to the server in a safe way, and then the storage mechanism is also safe because the data is encrypted. It can also be measured by how much time and money it takes to do something new.

For example: If an attacker wants to get personal information or do something else with the user's data, in this case, when a user uploads a file to a site, it is encrypted with AES so that the user's data can't be read by anyone. Because of this, if an attacker somehow gets the user-uploaded file, it won't work because the information was already encrypted when the file was uploaded. It's also possible that an attack may decrypt the encrypted file, in which case data would be safe from unauthorized access.

4.3 Pseudo code of ECC AND Proposed Hybrid Algorithms

	Algorithm for Generation Public Key Using ECC
First Step:	Choose any N number that you want to be the prime number.
Second Step:	Choose any number as n(x) for the purpose of generating the public key, where n(x)>n.
Third Step:	Calculate the point on the curve using the formula E, where E is E>n.
Fourth Step:	The formula for calculating the public key is $P = n(x) \times E$.
Fifth Step:	Choose any N number that you want to be the prime number.



Securing information in the cloud with Elliptic Curve Cryptography

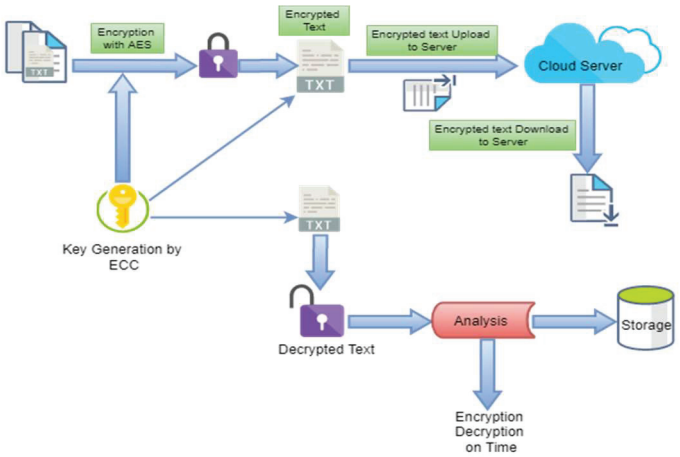


Figure 7 Proposed hybrid (ECC-AES) approach.

Algorithm for Encryption and Decryption Using the Advanced Encryption Standard (AESs)	
First Step:	To open the input file.
Second Step:	Insert the public key that was generated by ECC into the appropriated field.
Third Step:	AES encryption is applied to the input file with the help of the public key that was generated by ECC in step second.
Fourth Step:	After the AES encryption has been completed, the encrypted file is uploaded to the server.
Fifth Step:	Once the file has been uploaded, it will be downloaded to the server, where it will be translated using the public key provided by ECC, allowing the original file to be decrypted and returned.
Sixth Step:	The last step is to re-evaluate your situation. The combined effect of ECC and AES has a significant impact on the system's performance, as seen by the minimization of storage space and the strengthening of security services provided by the cloud server.

5 Implementation Results and Discussion

With the unique combination of ECC and AES, numerous cloud storage data are protected and secure connections are established for encryption and description of the information. This indicates that by using these two methods, the user will be able to decipher the original message. ECC and AES are shown to have advantages over RSA in the following section.

5.1 Merits of AES and ECC

In the cloud, Elliptic curve cryptography (ECC) is employed to protect the data. Maintaining data with a smaller key size might assist save storage space and achieve desired results. The RSA key size is 3072 bits. The ECC's best feature is its smaller key size and more efficient use of a public key to encrypt data [29]. In terms of data encryption and decryption accuracy and use of the most recent computational approaches, ECC outperforms RSA in this regard. Statistical analysis and cloud storage searching are only a few of the AES performance activities that are limited by cloud storage. For better cloud storage security, it's the most widely employed strategic algorithm. Everyone has the public key, which may be used to encipher and decipher any message [30]. In comparison to other cryptographic methods, ECC-AES offers superior security while using a smaller key size. Smaller key size saves memory and minimizes computing complexity. As a result, using a small key size is an effective way to secure data at a high level.

5.2 Comparison of Different Algorithms

It is necessary to examine and contrast the functionality and space optimization of different methods while using cloud storage [31]. As seen in Table 2, a comparison of several algorithms is provided. There are a variety of cryptographic methods based on a variety of variables. There have been comparisons of the performance of several cryptographic algorithms using various parameters, including the number of keys utilized, key length, rounds, and other constraints.

5.3 Tools Used

For implementing the proposed algorithm, we used programming language Python, VS code editor which is run on operating system windows-10, 1-TB hard drive, 8 Gb RAM and as well as to test the effectiveness of our system.

Table 2 Comparison of various cryptographic techniques

Factor	RSA	DES	3DES	Blowfish	Proposed Hybrid Approach (ECC-AES)
Number of key uses	2	1	1	1	1
Size of key in bits	1024	56	112–168	32–448	64–256
No. of rounds	1	16	48	16	10
Attacks and Limitation	Key generation week	Brute force	Computational power	Key frequently changing	Brute force

The images were read using the Python package SimpleCV. Portable Network Graphics (PNG) was the image format used in our code and for plotting graph we use MS Excel. Many cloud storage data were secured in a unique and efficient manner by combining ECC and AES, increasing the system's uniqueness and efficiency. the encrypted data is transmitted across secure networks.

5.4 Data Size for Proposed Scheme

Due to the fact that images typically take more time than text data to encrypt and decrypt, our suggested approach was tested against 3 separate image datasets in order to compare it to other current approaches. This was done because images often require higher computation time over text. To see how different photographs function in different situations, it is necessary to take a variety of sizes. 2823, 3482, and 5890 image datasets were used in the experimentation. A comparison of encryption times for various techniques is shown in Figure 8.

Figure 8 compares the time it takes to encrypt data using various cryptographic techniques. The algorithm under consideration is a hybrid one. Because the hybrid ECC-AES strategy has a smaller key size, it takes less time to encrypt data than other methods. Additionally, the hybrid ECC-AES method combines the best features of both techniques, resulting in a more secure system that is more resistant to attack. Furthermore, the proposed algorithm's encryption time is significantly less than that of existing techniques. As the time required to encrypt data decreases, so does the computing

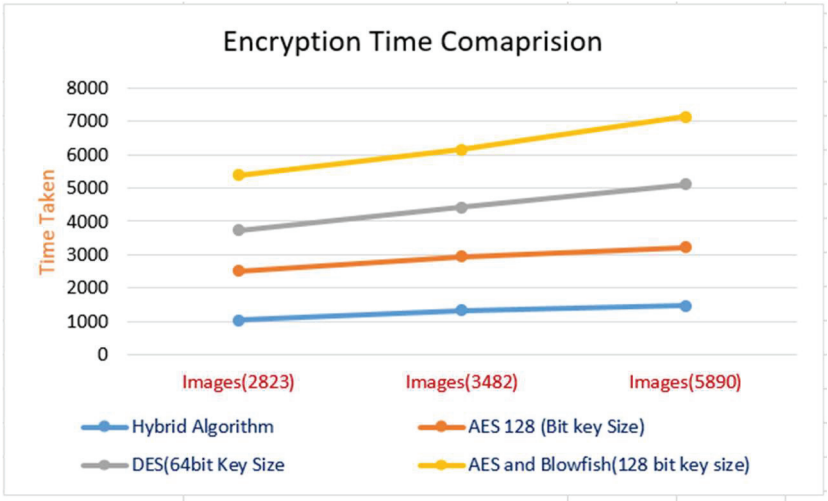


Figure 8 Encryption time comparison.

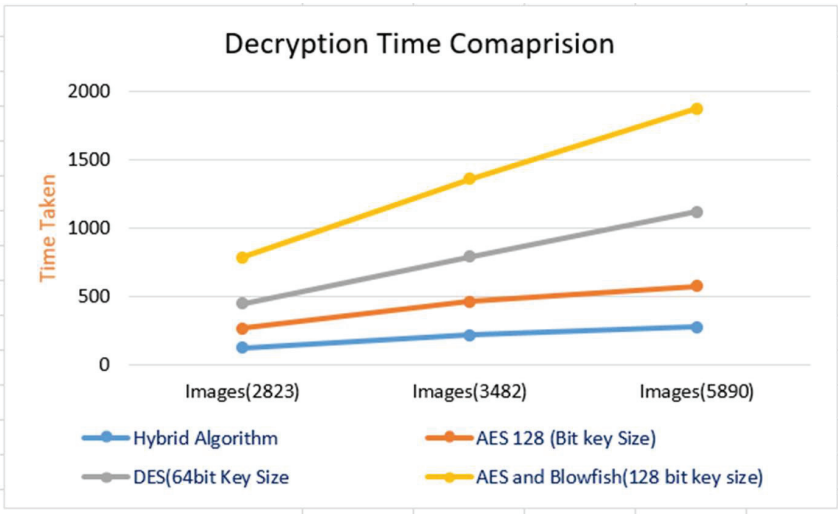


Figure 9 Decryption time comparison.

cost, making this method extremely efficient. As a result, we believe that our method is superior to others. Comparing the decryption times of various techniques is shown in Figure 9.

As seen in Figure 9, different encryption algorithms have varied decryption times. The hybrid algorithm is the one that was proposed for

implementation. Because of the reduced key size of the hybrid ECC-AES technique, it decrypts data faster than the current approaches. In addition, the hybrid ECC-AES algorithm combines the best features of both techniques, resulting in a system that is more resistant to assaults while still providing higher levels of security. Additionally, the suggested hybrid algorithm's decryption time is noticeably less than that of competing methods. Decryption takes less time and costs less money, thus it's a win-win situation. As a result, we believe that our method is superior to others.

5.5 Performance Evaluation

By using the technique of pairing up ASCII value as input to ECC, there is a significant decrease in the amount of time used by the algorithm but there will be little to no effect on the security since there are 2 more encryption layers protecting the original data.

As a whole, these are the outcomes:

- **Time:** The usage of combined encryption is projected to slightly enhance the total time required for encryption and decryption. Symmetric and Asymmetric ciphers are anticipated to require the same amount of time.
- **Space Complexity:** Because Image files are compressed prior to encryption and the keys employed are less in size, storage complexity for encrypted and source files is projected to be reduced.
- **Security level:** Due to the usage of a combination of symmetric and asymmetric ciphers, the security level is projected to be higher than that of current systems.
- **Avalanche effect:** The Avalanche Effect (AE) is a common way of evaluating how much an algorithm has changed over time. Text output can be significantly altered by even a modest change in input. By dividing the total number of modified bits in cypher bits by the number of all cypher bits, we can arrive to an AE value [32]. The formula we used to compute the Avalanche Effect of our suggested algorithm and the underlying article is as follows:

$$AE = \frac{\textit{No. of changed bits}}{\textit{Total no of bits}}$$

an algorithm with a greater than 50% avalanche effect has greater security power than the others. To demonstrate the system's superiority, our algorithm

Table 3 Comparison of avalanche effect

Encryption Algorithm	1-bit Key Change	Avalanche Effect	1-bit Plain Text Change	Avalanche Effect
Main paper	69	0.54	70	0.57
Blowfish	36	0.31	22	0.17
AES	64	0.6	69	0.54
Proposed work		0.56	84	0.64

Table 4 Energy consumption in encryption time (previous work)

Power Consumption (Watts)	DES	AES	Blowfish	Proposed Hybrid
Key size 64 bit	3.87W	3.41W	4.12W	**2.30W**
Key size 128 bit	4.01W	3.48W	4.38W	**2.42W**
Key size 92 bit	4.08W	3.52W	4.50W	**2.51W**
Key size 256 bit	4.38W	3.62W	4.28W	**2.58W**

Table 5 Energy consumption in decryption time (previous work)

Energy Consumption (Watts)	DES	AES	Blowfish	Proposed Hybrid
Key size 64 bit	3.2W	2.58W	3.78W	**1.30W**
Key size 128 bit	3.1W	2.78W	3.86W	**1.42W**
Key size 92 bit	3.28W	2.82W	4.40W	**1.51W**
Key size 256 bit	3.48W	3.06W	4.22W	**2.08W**

has the maximum Avalanche impact. Table 3 shown how the Avalanche effect works for different encryption algorithms.

5.6 Energy Consumption

Authentication systems rely largely on encryption techniques to protect their users' identities. Despite the fact that these technologies consume a lot of resources like CPU time, memory, and battery power, they have some drawbacks. Furthermore, cloud resources are dedicated to specific tasks. Watts are a convenient unit of measurement for the amount of power available. Table 4 shows the power consumption of the relevant systems in watts. A comparison was made between our suggested algorithm and the Base Paper approach in terms of the amount of energy required to decrypt a message measured in Watts.

Our proposed technique was compared to Base Paper's decryption time in Watts in Table 5.

6 Conclusion

Cloud computing and other IT-related services are effective regardless of the user's expertise of technology. Third-party cloud service providers can be utilized to store, manage, improve, and access data remotely from anywhere. Cloud service users have several options. User refers to someone who makes use of a service provided by a cloud provider. Services are offered at a reasonable cost, making it possible for a large number of people to access their data from any location. Because you don't have to bring your device with you while using cloud services, you can access them from anywhere. Because of this low data security that can only be addressed with unique tactics and must be secured by cloud service providers, cloud services are not without their drawbacks. ECC is specifically utilized to reduce the operations' complexity during the key generation process. ECC's improvement is superior to that of other cryptographic approaches because of its small-key size. When used in conjunction with ECC, AES can significantly improve data optimization and security. As cloud computing continues to grow, so does the need for additional security measures, such as cryptographic algorithms. The hybrid technique can be enhanced in the future by strengthening its security. The system's productivity and efficiency can be improved by adding more security levels.

Abbreviations

ECC: Elliptic curve cryptography, **AES:** Advance encryption standard, **DES:** Data encryption standard, **AE**: Avalanche effect, **RSA**: Rivest Shamir and Adleman.

Acknowledgements

Not applicable.

Competing interests

The authors declare that they have no competing interests.

References

[1] Daemen, Joan, Rijmen, Vincent. (March 9,), AES Proposal: Rijndael. National Institute of Standards and Technology 2003; p. 1. Retrieved 21 February 2013.

[2] Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation-Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering December 2011; vol. 1(2), pp. 6–12.

[3] Shukla, D.K.; Dwivedi, V.K.; Trivedi, M.C. Encryption algorithm in cloud computing. Mater. Today Proc. 2020, 37, 1869–1875.

[4] Yahia, H.S.; Zeebaree, S.R.M.; Sadeeq, M.A.M.; Salim, N.O.M.; Kak, S.F.; Al-Zebari, A.; Salih, A.A.; Hussein, H.A. Comprehensive survey for cloud computing-based nature-inspired algorithms optimization scheduling. Asian J. Res. Computer. Sci. 2021, 1–16.

[5] Qazi, R.; Khan, I.A. Data security in cloud computing using elliptic curve cryptography. Int. J. Computer. Communication. Network. 2019, 1, 46–52.

[6] Chen, Y.; Liu, H.; Wang, B.; Sonompil, B.; Ping, Y.; Zhang, Z. A threshold hybrid encryption method for integrity audit without trusted center. J. Cloud Comput. 2021, 10, 3.

[7] Sridharan, S.; Arokiasamy, A. Effective secure data storage in cloud by using ecc algorithm. Middle-East J. Sci. Res. 2017, 25, 117–127.

[8] Abdullahi Ibrahim, A.; Cheruiyot, W.; Kimwele, M.W. Data security in cloud computing with elliptic curve cryptography core. Int. J. Comput. 2017, 26, 1–14. Available online: http://ijcjournal.org/ (accessed on 22 October 2021).

[9] Manaa, M.E.; Hadi, Z.G. Scalable and robust cryptography approach using cloud computing. J. Discret. Math. Sci. Cryptogr. 2020, 23, 1439–1445.

[10] Madhavi, G.; Samatha, J. Secure data storage and access of data in cloud using Elliptic curve cryptography. IEEE J. 2020, 11. Available online: www.jespublication.com (accessed on 20 December 2021).

[11] Zhu, Y.; Fu, A.; Yu, S.; Yu, Y.; Li, S.; Chen, Z. New algorithm for secure outsourcing of modular exponentiation with optimal checkability based on single untrusted server. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.

[12] S.M. Celestin, V.K. Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. IEEE International Conference on Advanced Computing Dec 2009; pp. 82–85.
[13] Hafid Mammass and Fattehallah Ghadi, Implementation of Smartcard Personalization Software. International Journal of Future Generation Communication and Networking 2012; vol. 5(4). pp. 39–54.
[14] F. Amounas and E.H. El Kinani, A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin 1/2 Matrices. International Journal of Information & Network Security (IJINS) 2013; vol. 2(3), pp. 190–196.
[15] Md. Zaheer Abbas, Dr. JVR Murthy, Authenticated And Policy – Compliant Source Routing. International Journal of Engineering Research and Applications (IJERA) 2012; vol. 2(3), pp. 1347–1352.
[16] Bruce Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings. Springer-Verlag: 191–204. Archived from the original on 2014-01-26.
[17] "Cryptography: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Schneier on Security. Archived from the original on 2016-03-04. Retrieved 2015-12-31. (Wikipedia).
[18] Arockia, P.; Dharani, N.; Aiswarya, R.; Shailesh, P. Cloud data security using elliptic curve cryptography. Int. Res. J. Eng. Technol. 2017, 4, 32–36.
[19] Li, Y.; Gai, K.; Qiu, L.; Qiu, M.; Zhao, H. Intelligent cryptography approach for secure distributed big data storage in cloud computing. Inf. Sci. 2017, 387, 103–115.
[20] Saeed, Z.R.; Ayop, Z.; Azma, N.; Rizuan Baharon, M. Improved cloud storage security of using three layers cryptography algorithms. Int. J. Comput. Sci. Inf. Secur. 2018, 16, 34–39.
[21] Al-Dhuraibi, Y.; Paraiso, F.; Djarallah, N.; Merle, P. Elasticity in cloud computing: State of the art and research challenges. IEEE Trans. Serv. Comput. 2017, 11, 430–447.
[22] Hodowu, D.K.M.; Korda, D.R.; Ansong, E.D. An enhancement of data security in cloud computing with an implementation of a two-level cryptographic technique, using AES and ECC algorithm. Int. J. Eng. Res. Technol. 2020, 9, 639–650.
[23] Zhu, Y.; Fu, A.; Yu, S.; Yu, Y.; Li, S.; Chen, Z. New algorithm for secure outsourcing of modular exponentiation with optimal checkability based on single untrusted server. In Proceedings of the 2018 IEEE

International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.

[24] Agrahari, V. Data security in cloud computing using cryptography algorithms. Int. J. Sci. Dev. Res. 2020. Available online: www.ijsdr.org (accessed on 22 October 2021).

[25] Selvam, J.M.; Srivaramangai, P. Time complexity analysis of cloud authentications and data security: Polynomial based hashing and elliptic curve cryptography. Int. J. Anal. Exp. Modal Anal. 2020, 12, 850–860.

[26] Awad, W.S. A framework for improving information security using cloud computing. Int. J. Adv. Res. Eng. Technol. 2020, 11, 264–280.

[27] Astuti, N.R.D.P.; Aribowo, E.; Saputra, E. Data security improvements on cloud computing using cryptography and steganography. IOP Conf. Series Mater. Sci. Eng. 2020, 821, 012041.

[28] Manaa, M.E. Data encryption scheme for large data scale in cloud computing. J. Telecommun. Electron. Comput. Eng. 2017, 9, 1–5. Available online: https://jtec.utem.edu.my/jtec/article/view/2759 (accessed on 22 October 2021).

[29] Suresha, R.G. Enhancing security in cloud storage using ecc algorithm. Int. J. Sci. Res. 2013, 2–8. Available online: https://www.ijsr.net/archive/v2i7/MDIwMTM3NA==.pdf (accessed on 22 December 2021).

[30] Abbas, S.; Maryoosh, A.A. Improving data storage security in cloud computing using elliptic curve cryptography. IOSR J. Comput. Eng. 2015, 17, 48–53.

[31] Barati, M.; Aujla, G.S.; Llanos, J.T.; Duodu, K.A.; Rana, O.F.; Carr, M.; Rajan, R. Privacy-Aware cloud auditing for gdpr compliance verification in online healthcare. IEEE Trans. Ind. Inform. 2021, 1.

[32] Mahto, D.; Yadav, D.K. RSA and ECC: A comparative analysis. Int. J. Appl. Eng. Res. 2017, 12, 9053–9061. Sridhar C. Iyer, R.R. Sedamkar, and Shiwani Gupta. "A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach", Procedia Computer Science, vol. 79, 2016. doi: 10.1016/j.procs.2016.03.038

Biographies

Sunil Kumar Received a bachelor's degree in computer engineering from RGPV University in 2009, a master's degree in computer engineering from RGPV University in 2014, and respectively. He is currently pursuing the philosophy of doctorate degree at the Department of Computer Engineering, National Institute of Technology Jamshedpur. His research areas include Lightweight cryptography, cloud-IoT security, Machine learning, and social network analysis. He has been serving as an ad hoc reviewer for IGI global – IJISP journals more than 20 research paper.

Dilip Kumar is working as Assistant Professor at the National Institute of Technology Jamshedpur, India. Completed B. Tech (CSE) from BIT Sindri, Jharkhand, M. Tech (Computer Science) from NIT Rourkela, and Ph.D. from National Institute of Technology Jamshedpur, India, Research experience is around 23 years, area of research includes Optimization Techniques, Heuristic Techniques, Machine Learning, IoT, Cloud Computing.