

## Financial information security using hybrid encryption technique on multi-cloud architecture

Mustafa Noori Rashid<sup>1</sup>, Leith Hamid Abed<sup>1</sup>, Waleed Kareem Awad<sup>2</sup>

<sup>1</sup>Department of Computer Systems, Technical Institute of Anbar, Middle Technical University, Baghdad, Iraq

<sup>2</sup>Department of Computer Science, Computer Science and Information Technology, University of Anbar, Ramadi, Iraq

### Article Info

#### Article history:

Received Apr 16, 2022

Revised Aug 8, 2022

Accepted Aug 24, 2022

#### Keywords:

AES

Big data

DDSP

Encryption

RSA

SA-EDS

Security

### ABSTRACT

One of the most severe issues in the cloud is security. In comparison to financial data, so it is extremely sensitive and must be safeguarded against unwanted access. We have developed a proposed system based on three different keys. We divided the data into insensitive, sensitive, and highly sensitive data. The data will be saved on a separate cloud server. The proposed system used different keys for encryption and decryption purposes. The elliptic curve cryptography (ECC) based distributed cloud-based secure data storage (DDSP) approach was proposed to provide secure large data based data protection across the different clouds. With DDSP technology, the ECC scheme has been used for encryption and decryption purposes. The cloud is used for simulation. The results of the tests reveal that the suggested DDSP system is safe and saves time regarding data retention and retrieval. To analyze performance, we compared the DDSP method with advance encryption standard (AES), blowfish, rivest shamir adleman (RSA), security-aware efficient distributed storage (SA-EDS), and attribute based encryption (ABE) based secure distributed storage (ASDSS). In terms of information retention and recovery, our methodology is quite effective because it requires less amount of time as compared to other strategies.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



### Corresponding Author:

Mustafa Noori Rashid

Department of Computer Systems, Technical Institute of Anbar, Middle Technical University

Al-Za'franiya City, Rusafa, 10074, Baghdad, Iraq

Email: mustafan@mtu.edu.iq

## 1. INTRODUCTION

Cloud computing has attracted the attention of various communities in society like researchers, banking, consumer, student, business, and government organizations [1]. Financial data requires security from hackers and avoiding cybercrime; cloud computing technology is a transformative digital solution that provides the banking industry with unequaled levels of agility, confidentiality, and portability while increasing its ability to handle massive volumes of data [2]. In order to fulfill an agreement to provide certain services, "the cloud," which is a distributed and parallel computing platform, is employed in conjunction with network access on demand. The internet and its associated computer networks make up a cloud, and its datacenters handle the necessary hardware and software to mainly carry out computational and storage functions [3], [4]. The proposed algorithm is efficient enough to allow financial service organizations to ensure the protection of sensitive data by utilizing resources in a very convenient and dynamic manner. As demonstrated in Figure 1, cloud computing simply means that retrieving data from one computer to another over networking is simple and quick.

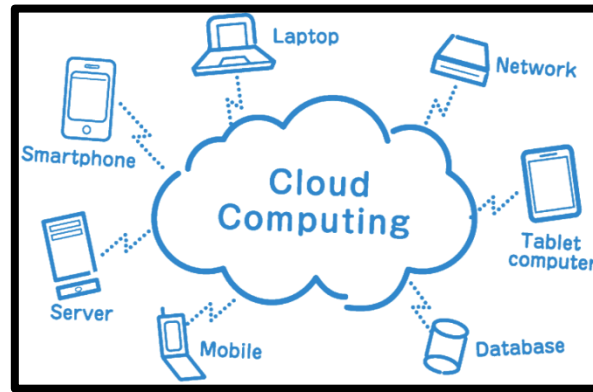


Figure 1. Cloud computing: an overview [5]

Dropbox, box, and sugar sync are examples of hybrid systems that collect an online synced version of your files. They also synchronize these files with local storage. The cloud computing experience relies heavily on synchronization. Furthermore, computing in the cloud is defined as a group of people with various systems that requires the same synchronized data. A decade ago, an IT project or startup required stable and internet-connected computing resources for multiple datacenters [6].

The rise of cloud data repositories and cloud computing is accelerated that paves way for big data to emerge. The use of the same technology to co-modify data storage and calculation time is known as cloud computing. It has a number of important advantages over traditional physical deployments. Not only that, but cloud platforms come in a variety of shapes and sizes, and they're occasionally coupled with traditional systems. It represents a deadlock for decision-takers in charge of large data projects [7]. Under what ways or which services of cloud computing would be the ideal fit for your computing needs, especially if you're working on a big data project? as illustrated in Figure 2, where huge data and its characteristics are displayed, these preparations frequently indicate bursting [8], fluctuating or storage requirements, and massive computational power. Profitable stakeholders visualize low-cost solutions and self-sufficient project outcomes and products.



Figure 2. Big data [9]

Big data is the phrase that refers to data volumes that are so massive and complicated that traditional applications are unable to handle them. New difficulties involve data collection, curation, search, and sharing of information storage, transport, visualization, and privacy [10]. Big data typically deal with large amounts of information gathered from multiple sources, which can lead to issues such as heterogeneity, which is currently being investigated. Resource allocation, scalability migration, cloud load balancing, and other issues are currently being researched.

A lot of privacy concerns arise from data gathering, including the use of analytical tools to extract data. As data is fake and spreads around the globe, ensuring privacy, and data security has become extremely difficult. Analytics regularly mine users' sensitive data that includes energy depletion, medical proceedings,

online behavior, supermarket records, and so on, inspection of this data reveals concerns about summarizing, perception, loss of control, and elimination [11].

Big data refers to massive amounts of data with unusual velocities and a wide range. The latter takes into account the large and varied amount of data generated by numerous assets that are self-sufficient [12]. Massive amounts of data are delivered in the direction of massive database management systems (DBMS) with different speeds and with different codes via a few different sources. It is because each data creditor chooses their methods or schemata for statistics files, and the nature of each package leads to different factual information. Working with a large number of entries and different speed costs seems to be a difficult issue that big data structures should handle [13].

Loss of data could result in a loss of value. In the event of a dangerous or critical accident, such as floods, earthquakes, or fires, statistical losses should be kept to a minimum. To meet these criteria, information should be available quickly in the event of an incident, with little disruption and loss. Despite the fact that it is a vital issue, there is a noticeable lack of research in this field [14].

## 2. PROPOSED METHOD

### 2.1. Literature review

Proposed a solution for secure communication between IoT devices and a distant server using lightweight elliptic curve encryption (ECC). ECC-constrained application protocol (ECC-CoAP) was the recommended CoAP implementation for IoT network authentication. Analysis of cryptographic threats confirmed ECC-safety CoAP's capacity. All assaults were well-defended. This method addresses important management and security concerns in IoT systems with minimal resources [15]-[17].

Suggested a problem with Bluetooth security, specifically secure easy pairing, utilizing a four-user authenticated key (4UAK) using ECC. The research covers secure simple pairing (SSP) with ECC design, implementation, and performance assessment (ECC). Using end-to-end latency, packet loss rate, throughput, the performance and security of a Bluetooth-based protected, and easy pairing idea were tested using ECC [18].

Created an asymmetric multiple-image encryption technique using ECC and a response code. The cipher-text picture was decrypted digitally. Asymmetric encryption employs public and private keys. The method can encrypt 16 photographs simultaneously. Simulations showed the encryption scheme's effectiveness and resilience. Using image histogram, correlation of neighboring pixels, information entropy, and key space analysis, the system proved resistant to a range of assaults [19].

A three-factor remote user authentication mechanism based on ECC was suggested to secure the communicating user's privacy and data confidentiality. Investigated many cryptographic attacks. The suggested system is impervious to such assaults. A comparison of the proposed scheme's computation and communication overheads with other existing protocols showed that it was lightweight and successful [20].

Built an anonymous authentication mechanism for wireless body area networks (WBAN), pointing up security weaknesses including known session-specific temporary information (KSSTI), insider, and clock synchronization issues. The project aimed to provide a lightweight ECC-based authentication mechanism for the internet of medical things (IOMT). The protocol's rivals were examined on security, compute, storage, and communication costs. The findings showed that the suggested protocol was more resilient and could be implemented more easily [21].

Deliberated Rivest–Shamir–Adleman (RSA) asymmetric cryptography system. It tries to show the domains of RSA technique used in public networks, wireless sensor networks, picture encryption, cloud computing, proxy signature, IoT, and embedded devices. So analyzed RSA scheme trends and performance parameters such as security, speed, efficiency, computational complexity, and space. This study also described the scheme's methodology and strengths [22], [23].

Offered physical space on a variety of storage devices to speed up Internet data transfer while encrypting and hiding it from outsiders. The research uses hybrid data compression to enhance the quantity of data to be encrypted using RSA encryption. Lossy and lossless Steganography might also be used. The study's results were compared to similar industries. The algorithm's visual quality and storage capacity were tested well. The algorithm's security and attack resistance beat the competition [24].

A gravitational search algorithm (GSA) based ECC-dependent picture encryption technique was suggested. ECC's private key generation stage utilized GSA to optimize image encryption. Photo output, like peak signal to noise ratio (PSNR), is employed as just a validity feature in the optimization phase, demonstrating the suggested approach's usefulness. The recommended encryption approach provides better PSNR values than ECC. Image encryption allows users to send digital photos wirelessly while ensuring privacy and authenticity [25].

Provided a detailed review of cryptography, encryption, decoding, and RSA public key cryptography, as well as relevant military, commercial, privacy, and information security applications. Personal weaknesses in RSA information security were questioned. The research examined RSA and cryptographic system fundamentals. Based on RSA cryptography and its uses, new software to improve the RSA algorithm was released [26].

Studied data encryption standard (DES) private and RSA public techniques. Both methods' ability to encrypt and decode plaintext quickly was their defining characteristic. Encryption and decryption throughput was also considered. Finally, a formula for calculating encryption and decryption throughput was found [27].

A cryptographic technique might boost security for vehicle over-the-air updates. Attribute based encryption (ABE) protected over-the-air software upgrades. State of the art alternatives lacked this feature. ABE may incorporate into over the air (OTA) update procedures while conforming to automotive design and documentation requirements. The study found low-cost ways to boost security [28].

## 2.2. Problem definition

The cloud's security has long been a major worry, and stored data in a cloud can be readily accessed by spammers. Your personal information is accessible to them. To ensure security for massively scattered data in multiple clouds, especially financial data therefore the suggested study proposes an ECC-based safe shared storage mechanism for big data in cloud storage (DDSP).

## 3. METHOD

### 3.1. Data division

The encryption techniques secure confidential information and reduce the chances of unauthorized access. These strategies ensure that data is secure and that it is divided into separate groups. Then different keys are used to encrypt the input and stored the data in the database. The data is split into three parts based on its sensitivity, which is sensitive, less sensitive, and highly sensitive as explained in Figure 3. Then, the encryption key is used on sensitive, less sensitive, and highly sensitive data. Encryption techniques provide security and improvement for cloud-based distributed storage.

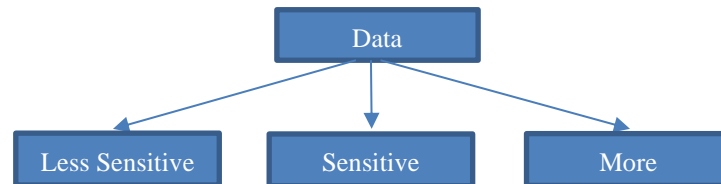


Figure 3. Data division

### 3.2. Provide security to distributed cloud storage based on ECC

Using this proposed technology, the storage is supplied with high-level security. The input data is split into three parts namely sensitive, less sensitive, and highly sensitive. Then, the input data is allotted to its sensitivity level. Based on the data sensitivity level, different keys are applied. The very strong key is used for the most sensitive data. In this step, encryption techniques such as advance encryption standard (AES), rivest shamir adleman (RSA), and ECC are used for the less sensitive, sensitive, and more sensitive data. After that, the data is stored on cloud storage as demonstrated in Figure 4. The encrypted data is then decrypted using decryption. The keys are used to decrypt data that is kept in the cloud. Finally, we combine the decrypted data with the original data to obtain the original data. There are three stages to the process:

- Phase 1: the data is separated into three groups in phase 1, namely: sensitive data, less sensitive data, and extremely sensitive data. Information that is more sensitive, such as user ids and passwords, is classified as highly sensitive data. The encryption algorithm is applied to data using the keys. Based on the data sensitivity level, AES is used for less sensitive, RSA is for sensitive, and ECC is used for highly sensitive data. Encryption techniques are used to secure the data before sending it to the database.
- Phase 2: in phase 2, the encrypted data is stored on the cloud storage, which is encrypted with different keys.
- Phase 3: in this phase, the ciphertext will convert into a readable format. By using the same keys that we used for the encryption time, the decryption technique is performed. Once the decryption is done, we now merge the data and get the original data, which is secured.

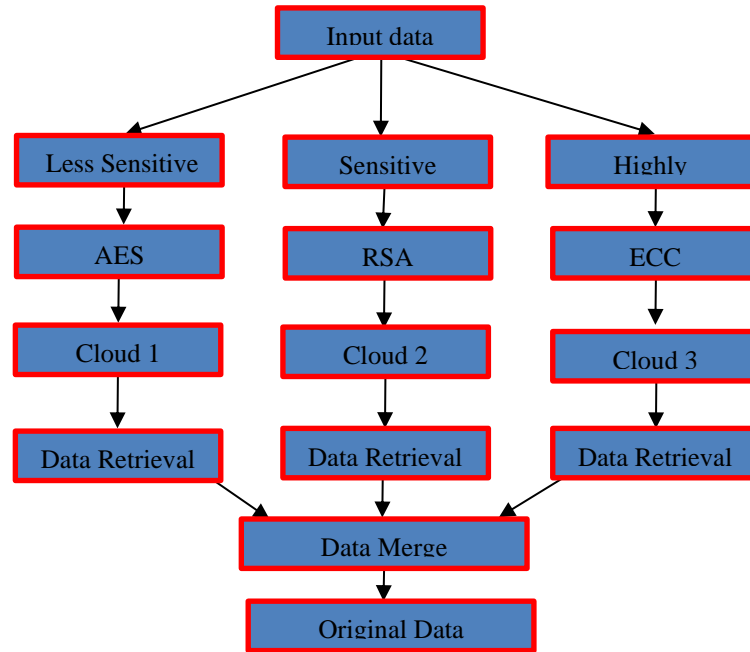


Figure 4. DDSPE's flowchart

### 3.3. Distribution of data and encryption algorithm

The encryption approach divides the data into three categories: sensitive, less sensitive, and more sensitive. The data is distributed by dividing it into groups based on its labels. The inputs include name of data (NOD), a list of more sensitive data (list 1), and a list of sensitive data (list 2). N are the names of the label of each NOD. After the distribution of data, the output includes the different names of data based on their sensitivity level. Algorithm 1 shows the pseudo-code of the distribution of data and encryption algorithm. Following are the steps of algorithms:

Step 1: Lists of data are used as input (List 1, List 2). List1 contains highly sensitive data, List2 contains sensitive data, and List3 contains the data's searchable name.

Step 2: For each NOD, search every label of the information and see if it corresponds to List 1 or List 2 or not.

Step 3: If the data is found in List 1, the data will be encrypted using the ECC algorithm.

Step 4: If the data is found in List 2, the data will be encrypted using the RSA algorithm.

Step 5: Otherwise, the data will be encrypted using the AES algorithm.

Step 6: All encrypted data is the output that includes a, b, c. The encrypted data is stored on different cloud storage.

Algorithm 1 distribution of data and encryption algorithm

Require: NOD, List1, List2

Ensure: s, a, b, c

1. Input NOD, List1, List2

2. READ: data is read from the input source.

3. For  $\forall$  NOD do

4. For each name of data do

5. If a Li List 1 exists, then

6. Key1 is created using genKey (P, Q, R)

7. Execute ECC algorithm for the encryption of data with Key1

8. Create a

9. Else if a Li List 2 is present, then

10. Key2 is created using genKey (P, Q, R)

11. Execute RSA algorithm for the encryption of data with Key2

12. Generate b

13. Else

14. Generate random Key3

15. Do AES operation for the encryption of data using Key3

16. Generate y

17. End if

18. End for

19. Generate S values

20. End for

21. Output a, b, c

### 3.4. Algorithms for data retrieval

The original data will be retrieved using this algorithm that is distributed in Algorithm 1. The algorithm's inputs are a, b, c, key1, key2, and key3. Then, the algorithm gives the output S. Algorithm 2 shows the pseudo-code. Following are the steps for the algorithm of data retrieval:

Step 1: In step1, the encrypted data will be the input that we got from Algorithm 2. Then the keys will be required to decrypt the data that is stored in a register.  
 Step 2: Initialize a few datasets d, d', d'' used for the storage of data after decryption.  
 Step 3: Decrypt the data using the algorithm and generated keys.  
 Step 4: To get the original data, after the decryption of data, merge all the data.  
 Step 5: And the original data will be the output.

Algorithm 2 data restoration algorithm

Essential: a, b, c, Key1, Key2, Key3

Ensure: S

1. Input a, b, c, Key1, Key2, Key3
2. Initialize d←0, d' ←0, d'' ←0
3. /\* Inputs a, b, and c are received from several cloud servers \*/
4. d ← Decrypt a using Key1 with the ECC algorithm
5. d' ← Decrypt b using Key2 with the RSA algorithm
6. d'' ← d ⊕ Key3
7. S ← Combine d, d' and d'' to obtain original data
8. Output S

## 4. RESULTS AND DISCUSSION

### 4.1. Implementation

Python is a development, machine learning, and data science. It also has an extensive selection of libraries and frameworks. Python is an open-source popular language for cryptography. Python3 supports advanced techniques like artificial intelligence, machine learning, and deep learning. Libraries used:

- Pyaes: it is a pure-python implementation of the AES block-cipher algorithm.
- Pbkdf2: it is an algorithm based on passwords for key generation.
- Binascii: using this, binary gets converted to ASCII.
- Secrets: this library is used to generate random numbers to be cryptographically secure.

We have shown the results below all the encryption techniques. These algorithms ensure confidentiality and power key security initiatives such as authentication and integrity. Figure 5 shows the keys generated for encryption and decryption using AES. AES supports the largest bit size and is made unbreakable with the brute force method.

Date of birth	AES key
4/24/00	96485bdf985a6f4e139ba6fb96ee89f09c543a7a608fba5fc40846f42ecd04*
5/12/00	77551c13a9c7ccac74214eec22136d50ed9045da8cd9890cdf908a122876966*
3/3/00	3fbc1cd9da695f8cf1d553de712ff3d9e22f0207ab1d389947f57ad6f644d244*
11/5/00	5907d53df90fba8155d1431a2ff9c4fa30a8e041dccc6cf199c05b3d7a0e189f0*
6/17/00	bb31ed317ac39b1a68c91a0b12ca79fd379db1e2eee5c70189d3b4d95a232fd*
11/8/00	6b3f5e96863b5ddcc640af884676380e1c602af49b4b03f19364582cdf6a68c*
12/9/00	cf9ed1bb7968b20d3b3087c92277b02f18d152310d1e6838575791eccdde288*
1/21/00	7ae36c7bc691815c747947169af6e81966db8f9fad9226bf4809c7e02487ff0b1*
4/30/00	eb1d0eaa22bd08386a11eee18f72c0c1cf0759414273de1aafeff528d95dab62*
6/15/00	6ee5c70c2d1f98a0adfe5c2ba2b351b08caaf60ce7e14a0ed3c765d3a2607bc*
6/28/00	5f713fe1548b892502ef506c385d9c48b8a4ab51a9b9c9300d351fde8a8fc79c*
12/17/00	ad5e0a8ae8acd7e34a293d7ad040a42f7e1253a8feed585f3ec82b889aaf227b*
8/21/00	00f77412fd2eb50459b3c7096aea2820df47fcec4f10db5b6597d56950303e4c*
9/16/00	2375a4635e677071bf2a2bb60fb9c6378118bc9f94050bd26f942de073b97116*
7/24/00	4530ed7b7784487a73631dc5e404bc2a022d4a68ac0e594df537003952fea749*
3/17/00	beadc1084ee8b6a6025b92d84403ba4f41ea7ffe5680a72c1bd3fe4c2d6426ce*
8/12/00	858a06f1032c72f2012637081969d87fd7f084ecbcbf9e712e0be1787161d59*
1/19/00	f195d32d1252340f422da5716a0c9dbfea5302ffedeb3aeb9bb149855e19120b*
9/28/00	36533d88bcecf7e0231ee0cf8de41da1389384979c68a0ea75cf0e67b9d53f6*
9/14/00	df6921ec950c3245df50847e0827eaa148f0553c1235dccc4c315f265985eac*
9/3/00	917f505830a630b530b32649e04f48f2d7f15efbc2d5aa555ff3aa8d1afd0b1e*
3/15/00	cc0ca5c631a64630642953c05c52378e76d8477cbec067cc189ac2926d0734*
3/18/00	24b74ba64c0ee96be27b7c771baef28019e34b6c90837177b4e7ddc1580cc3577*
11/15/00	

Figure 5. AES key generation

Figure 6 depicts AES-key generation for 128-bit. During the decryption and encryption processes, encryption and decryption schemes of AES are initialized and processed. Figure 7 shows both RSA's initialization and processing. Figure 8 illustrates both the encryption and decryption processes involved in the ECC scheme.

	Date of birth	AES key	AES Time
0	4/24/00	96485bdf985a6f4e139ba6fc0b96ee89f09c543a7a608fba5fc40846f42ecd04'	0.07144379615783691
1	5/12/00	77551c13a9c7ccac74214eec22136d50ed9045da0cd9890cdf9b8a122876966'	0.14203143119812012
2	3/3/00	3fbc1cd9da695f8cf1d553de712ff3d9622f0207ab1d389947f57ad6f644d244'	0.213155746645996094
3	11/5/00	5907d53df90fba8155d1431a2ff9c4fa30a8e041dccc6f199c05b3d7a0e189f0'	0.2911067088972168
4	6/17/00	bb316ed317ac39b1a68c91a0b12ca79fd379db1e2eee5c70189d3b4d95a232fd'	0.36206531524658203
5	11/8/00	6b3f55e96863b5ddcc6640af884676380e1c602af49b4b03f19364582cdf6a68c'	0.4333500862121502
6	12/9/00	cf9ed1bb7968b20d3b3087c92277b82f18d152310d1e6838575791ecccde288'	0.5031695365905762
7	1/21/00	7ae36c7bc691815c747947169af6e81966db8fefad9226f4809c7e02487ff0b1'	0.6175296306610107
8	4/30/00	eb10eaa22bd683aa11eee18f72c6c1cf0759414273de1aafeff528d95dab62'	0.688591718673786
9	3/16/00	6e5c70c2d1f98a0a6dfe5c2ba2b351b84caafc6c7e14a0ed3c765d3a2607bc'	0.7584307193756104
10	6/15/00	5f713fe1548b892502ef506c385d9c48b0a4ab51a9b9c9300d351fde8e8fc79c'	0.8290212154388428
11	6/28/00	ad3e0a8ae8acd7e34a293d7ad040a42f7e1253a8feed585f3ec82b889aaf2276'	0.8999667167663574
12	12/17/00	00f77412fd2eb50459b3c7096aea2820df47ffec4f10db5b6597d56958303e4c'	0.9781919655664062
13	8/21/00	2375a4635e677071bf2a2bb60fb9c6378118bc9f94050bd26f942de073b97116'	1.0463265953063965
14	9/16/00	4530ed7b7784487a73631dc5e484bc2a022d4a68ac0e594df537003952fea749'	1.111415147781372
15	7/24/00	beadc1084ee8b6a025b92d84403ba4f41ea7ffe506ca72c1bd3fe4c2d6426ce'	1.187971365308838
16	8/12/00	858a06f1032c72f2012637081969d87fd7f084ecbbc9e712e0be1787161d59'	1.2579741477966309
17	1/19/00	f195d32d1252340f422da5716a6c9dbfea5302ffedeb3aeb9bb149855e19120b'	1.398842917251587
18	1/19/00	366533d88bcecf7e0231ee0cf8de41da1389384979c68a0ea75cf0e67b9d53f6'	1.4675827026367188
19	9/28/00	df6921ec956c3245fd04d7e6827eaa148f0553c1235dccc4c315f265985eac'	1.5374970436096191
20	9/14/00	917f505830a630b530b32649e04f48f2d7f15efbc2d5aa555ff3aa8d1afd0b1e'	1.6067121028900146
21	9/3/00	cc0ead5c631a64630642953c05c52378e76d8477cbecc67cc189ac2926dc0734'	1.67661452293396
22	3/15/00		
23	3/18/00		
24	11/15/00	24b74ba4c0ee96be27b7c771baef28019e34b6c9037177b4e7ddc158bcc3577'	1.7470362186413885

Figure 6. AES key and process

	City	RSA Time
0	San Diego	1.0448269844055176
1	Thomson	1.045046329498291
2	San Diego	1.0452167907823486
3	Douglassville	1.0453801155098332
4	Licking	1.0455405712127686
5	Marion	1.0457017421722412
6	San Diego	1.0458600521087646
7	San Diego	1.0460197925567627
8	Sheboygan	1.0461974143981934
9	San Diego	1.0463566780099332
10	San Diego	1.046513319015503
11	Dallas	1.0466704368591309
12	San Diego	1.0468273162841797
13	Valparaiso	1.0469839572986494
14	San Diego	1.0471389293678654
15	Tigard	1.047295093536377
16	Kalamazoo	1.0474495887756348
17	San Francisco	1.0476062297821045
18	San Diego	1.0477635860443115
19	Los Angeles	1.0479207838879395
20	San Diego	1.04807710647583
21	San Diego	1.0482332706451416
22	San Diego	1.0483894348144531
23	Albany	1.048545360561855

Figure 7. RSA process

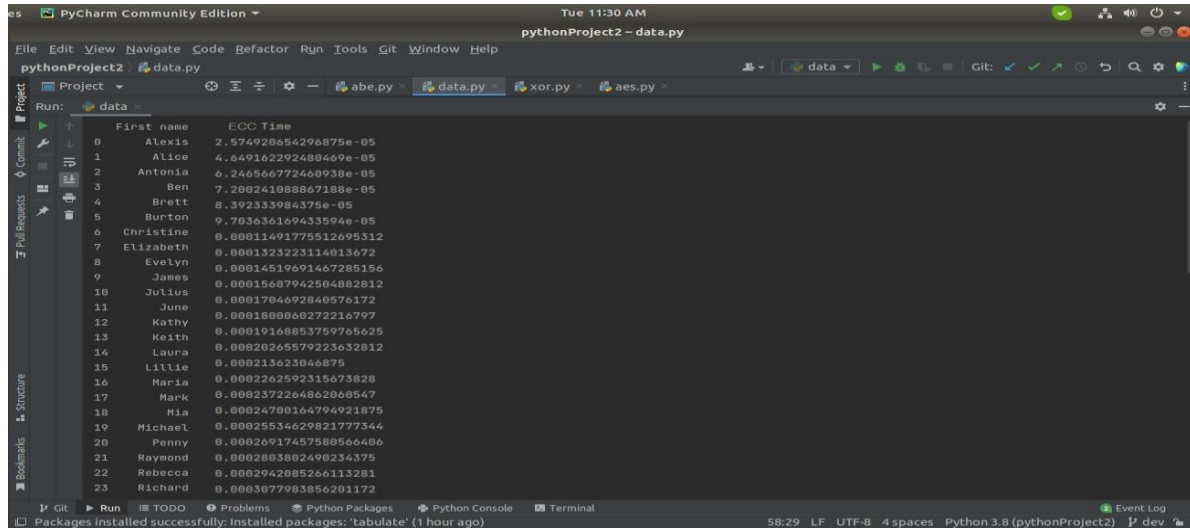


Figure 8. ECC process

4.2. Discussion and results of simulation

CloudSim toolkit 3.0.3 was used along with Eclipse as an integrated development environment (IDE). Java 1.8 was used as a platform for implementing the proposed scheme, DDSPE. We used financial data in this example as input data and encrypted it, then stored it on a cloud. For the distribution of data and encryption, Algorithm 1 was executed and its implementation was shown in Table 1. For the retrieval of data, Algorithm 2 was executed. It is clearly visible from the results of the experiment that the proposed technique consumed a short time for the storage and retrieval of data in different formats like gigabyte (GB), megabyte (MB), and kilobyte (KB). The comparisons were made between DDSPE and security-aware efficient distributed storage (SA-EDS). DDSPE proved that it consumed less time in storing and retrieving the data GB, MB, and KB. Figure 9 shows that DDSPE consumes less time to store the data as compared to other methods. Hence, the more efficient technique is DDSPE.

Table 1. Key of type’s techniques

Methods	Key Length (BIT)
ECC	12
ABE	50
AES	66
BLOWFISH	34
RSA	50

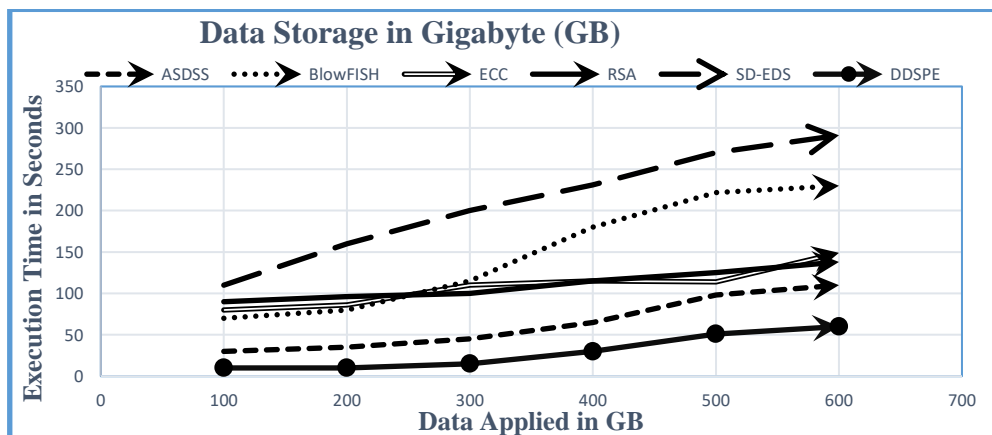


Figure 9. A comparison of the many forms of data storage and data retrieval of DDSPE, SA-EDS, ECC, blowfish, RSA, and ASDSS in GB



Figure 10 shows the data storage in MB and DDSPE’s comparison with other methods in terms of execution time. Figure 11 shows comparison of DDSPE with other approaches. It shows that DDSPE gives better performance when it is compared with blowfish, AES, RSA, and ECC. DDSPE consumes less time to store the data in KB. Figure 12 shows the comparison of DDSPE with the other methods. It shows that DDSPE gives better performance when it is compared with RSA, blowfish, AES, and ECC. DDSPE consumes less time to retrieve the data in GB.

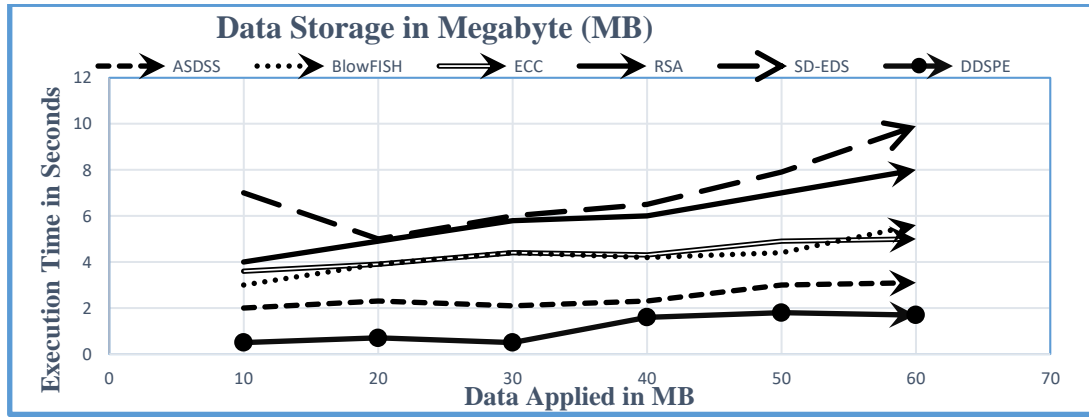


Figure 10. A comparison of the various storage options spaces of data of DDSPE with other methods in MB

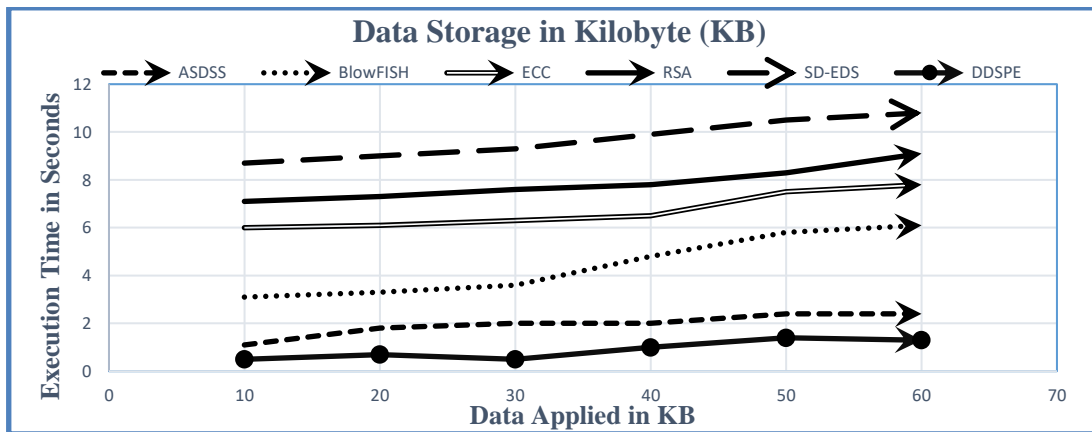


Figure 11. Data storage DDSPE comparison with another approach in KB

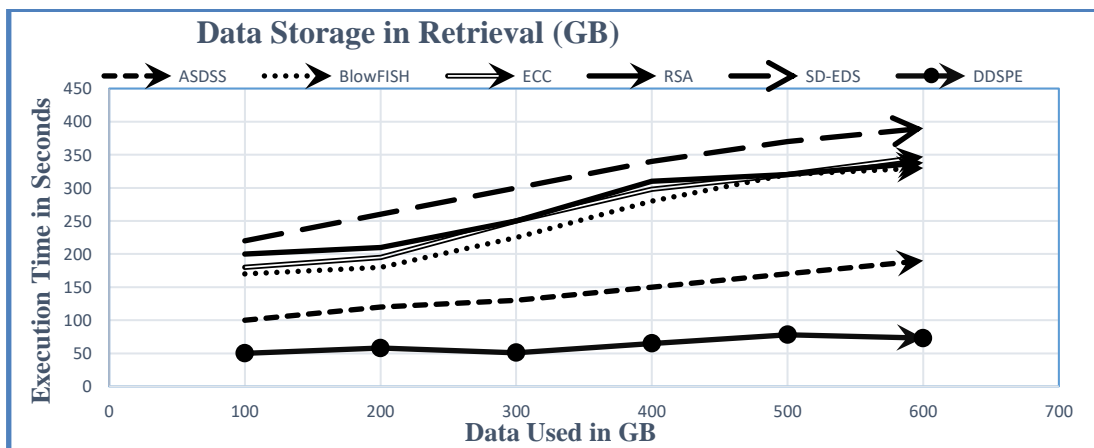


Figure 12. DDSPE and other methods data retrieval comparison in GB

Figure 13 shows the comparison of DDSPE with the other methods. It shows that DDSPE gives better performance when it is compared with RSA, blowfish, AES, and ECC. DDSPE consumes less time to retrieve the data in MB.

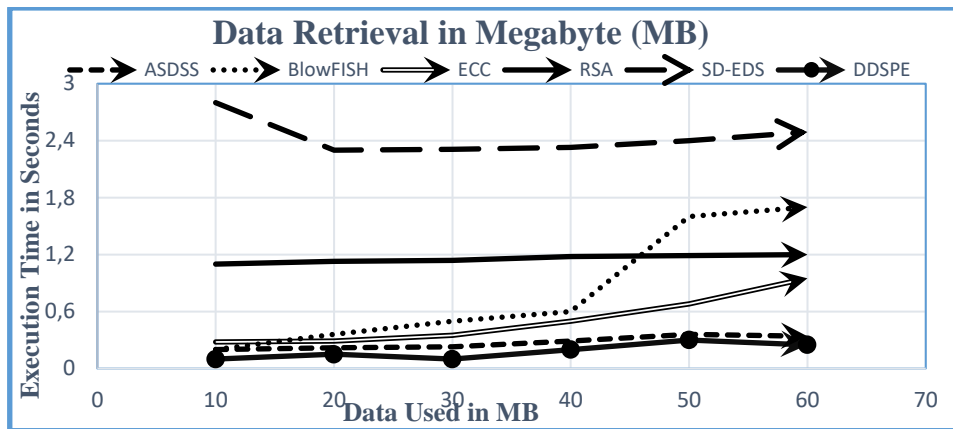


Figure 13. DDSPE and other methods data retrieval comparison in MB

Figure 14 shows the comparison of DDSPE with the other methods. It shows that DDSPE gives better performance when it is compared with RSA, blowfish, AES, and ECC. DDSPE consumes less time to retrieve the data in KB format.

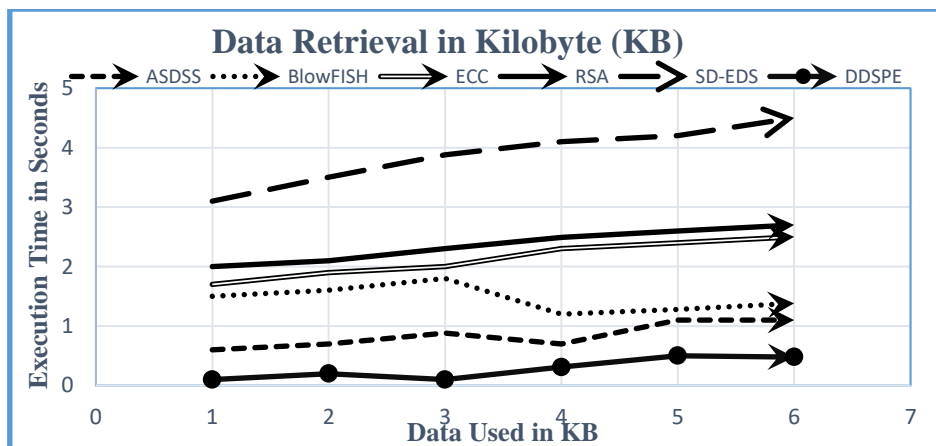


Figure 14. DDSPE and other methods data retrieval comparison in KB

### 5. CONCLUSION

A variety of methods have been tested over last three decades for safety purposes by many scientists. Many new methods have also been tested and developed in different parts of the world with the use of multiple methods of cryptography and various algorithms for encrypting data. No algorithm has yet been shown to be completely safe. Cloud computing enables complete storage, network access, accounting, consumer applications, and businesses. Cloud computing has a lot of cool benefits such as much-needed user, pay per use, shared pool calculations, fast expansion, and desired services. Cost savings are a huge benefit to the cloud. Cloud security is a main limitation faced by user in cloud. Storing the data on a cloud server is a huge difficulty. The user does not have complete control over their data on the cloud. Many encryption solutions rely on passwords to keep the server secure. Large data collection is a cloud computing strategy for dealing with high-level storage rather than security concerns like availability, reliability. As the bulk of the data grows larger, system integration gets more complex. Safety is a fundamental problem in modern security. The data sync problem only occurs in huge storage due to computer resource constraints. Data is

stored in the same cloud in a present system, and therefore only a single key is used for decryption and encryption. This program's data might be readily hacked. As a result, the DDSPE system is presented as a solution to this problem. In this case, the input is still divided into three pieces (based on its sensitivity level), every component is encoded with AES, SA-EDS, ECC, RSA, blowfish, and ASDSS, among other approaches. These bits of data would be encrypted and stored on separate cloud servers, with keys required to retrieve, decrypt data. As a result, our technique outperforms SA-EDS, AES, blowfish, and RSA related to data preservation and retrieval efficiency. In comparison against SA-EDS, AES, ASDSS, blowfish, and RSA techniques, DDSPE requires less time to recover data in MB, KB, and GB.





## REFERENCES

- [1] S. Pronika and S. Tyagi, "Performance analysis of encryption and decryption algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 2, pp. 1030–1038, Aug. 2021. doi: 10.11591/ijeecs.v23.i2.pp1030-1038.
- [2] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," *IEEE Access*, vol. 9, pp. 57792–57807, 2021, doi: 10.1109/ACCESS.2021.3073203.
- [3] M. Patel, A. Mehta, and S. Patel, "Container migration and placement in hybrid cloud-fog environment: systematic review," *International Journal on "Technical and Physical Problems of Engineering" (IJTPE)*, vol. 50, no. 50, pp. 130–135, Mar. 2022, [Online]. Available: <http://www.iotpe.com/IJTPE/IJTPE-2022/IJTPE-Issue50-Vol14-No1-Mar2022/19-IJTPE-Issue50-Vol14-No1-Mar2022-pp130-135.pdf>.
- [4] C. Clark *et al.*, "Live migration of virtual machines," *Proceedings of the 2<sup>nd</sup> conference on Symposium on Networked Systems Design & Implementation*, vol. 2, pp. 273–286, 2005. [Online]. Available: [https://www.usenix.org/legacy/events/nsdi05/tech/full\\_papers/clark/clark.pdf](https://www.usenix.org/legacy/events/nsdi05/tech/full_papers/clark/clark.pdf).
- [5] H. Pallathadka, G. Sekhar, K. Phasinam, M. Ritonga, and M. Naved, "An investigation of various applications and related challenges in cloud computing materials today: proceedings an investigation of various applications and related challenges in cloud computing," *Materials Today: Proceedings*, vol. 51, pp. 2245–2248, Dec. 2021, doi: 10.1016/j.matpr.2021.11.383.
- [6] R. Basmadjian, H. D. Meer, R. Lent, and G. Giuliani, "Cloud computing and its interest in saving energy: the use case of a private cloud," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, no. 1, pp. 1–25, Jun. 2012. doi: 10.1186/2192-113X-1-5. [Online]. Available: <https://link.springer.com/article/10.1186/2192-113X-1-5>.
- [7] I. Odun-Ayo, O. Alagbe, and J. Yahaya, "A systematic mapping study of security, trust and privacy in clouds," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1598–1610, Jun. 2021, doi: 10.11591/eei.v10i3.1887.
- [8] S. Kaisler, F. Armour, and J. A. Espinosa, "Introduction to big data: challenges, opportunities, and realities minitrack," *2014 47<sup>th</sup> Hawaii International Conference on System Sciences*, 2014, pp. 728–728, doi: 10.1109/HICSS.2014.97.
- [9] V. Dutt and M. Payal, "A hybrid approach of big data with cloud applications for a hybrid approach of big data with cloud applications for detailing the different methodologies & efficiency," *Global Journal on Application of Data Science and Internet of Thingsno*, vol. 2, no. 1, pp. 13–24, May 2018.
- [10] M. I. Mihailescu and S. L. Nita, "Software engineering and applied cryptography in cloud computing and big data," *International Journal on "Technical and Physical Problems of Engineering" (IJTPE)*, vol. 7, no. 3, pp. 47–52, Sep. 2015, [Online]. Available: <http://www.iotpe.com/IJTPE/IJTPE-2015/IJTPE-Issue24-Vol7-No3-Sep2015/9-IJTPE-Issue24-Vol7-No3-Sep2015-pp47-52.pdf>.
- [11] C. Pilato *et al.*, "EVEREST: a design environment for extreme-scale big data analytics on heterogeneous platforms," *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021, pp. 1320–1325, doi: 10.23919/DATe51398.2021.9473940.
- [12] A. Yan, W. Wang, Y. Ren, and H. W. Geng, "A clustering algorithm for multi-modal heterogeneous big data with abnormal data," *Frontiers in Neurorobotics*, vol. 15, p. 64, Jun. 2021, doi: 10.3389/fnbot.2021.680613.
- [13] A. Castro, V. A. Villagrà, P. García, D. Rivera, and D. Toledo, "An ontological-based model to data governance for big data," *IEEE Access*, vol. 9, pp. 109943–109959, 2021, doi: 10.1109/ACCESS.2021.3101938.
- [14] V. Chang, "Towards a big data system disaster recovery in a private cloud," *Ad Hoc Networks*, vol. 35, pp. 65–82, 2015, doi: 10.1016/j.adhoc.2015.07.012.
- [15] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867–1896, Feb. 2021, doi: 10.1007/s11277-020-07769-2.
- [16] A. Ayoub, R. Najat, and A. Jaafar, "A lightweight secure CoAP for IoT-cloud paradigm using elliptic-curve cryptography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 3, pp. 1460–1470, Dec. 2020, doi: 10.11591/ijeecs.v20.i3.pp1460-1470.
- [17] Z. Kasiran, S. Abdullah, and N. M. Nor, "An advance encryption standard cryptosystem in iot transaction," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 17, no. 3, pp. 1548–1554, 2020, doi: 10.11591/ijeecs.v17.i3.pp1548-1554.
- [18] D. H. A. Alfarjat, J. Hanumanthappa, and H. S. Hamatta, "Implementation of Bluetooth secure simple pairing (SSP) using Elliptic curve cryptography (ECC)," *International Journal of Computer Science & Network Security*, vol. 21, no. 3, pp. 60–70, 2021, doi: 10.22937/IJCSNS.2021.21.3.9.
- [19] W. Li, X. Chang, A. Yan, and H. Zhang, "Asymmetric multiple image elliptic curve cryptography," *Optics and Lasers in Engineering*, vol. 136, p. 106319, Jan. 2021, doi: 10.1016/j.optlaseng.2020.106319.
- [20] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *The Journal of Supercomputing*, vol. 77, no. 2, pp. 1114–1151, Feb. 2021, doi: 10.1007/s11227-020-03318-7.
- [21] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," in *International Journal of Information Security*, vol. 19, no. 1, pp. 129–146, Feb. 2020, doi: 10.1007/s10207-019-00464-9.
- [22] M. S. A. Mohamad, R. Din, and J. I. Ahmad, "Research trends review on RSA scheme of asymmetric cryptography techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 487–492, Feb. 2021, doi: 10.11591/eei.v10i1.2493.
- [23] M. S. Asaad and M. S. Croock, "Adaptive security approach for wireless sensor network using RSA algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, pp. 361–368, Apr. 2021, doi: 10.11591/ijeecs.v22.i1.pp361-368.





- [24] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding data using efficient combination of RSA cryptography, and compression steganography techniques," *IEEE Access*, vol. 9, pp. 31805–31815, 2021, doi: 10.1109/ACCESS.2021.3060317.
- [25] R. Navatejareddy, M. Jayabhaskar, and B. Sathyanarayana, "Elliptical curve cryptography image encryption scheme with aid of optimization technique using gravitational search algorithm," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 25, no. 1, pp. 247–255, Jan. 2022, doi: 10.11591/ijeecs.v25.i1.pp247-255.
- [26] X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption," *Proceedings of 2011 6th International Forum on Strategic Technology*, 2011, pp. 1118–1121, doi: 10.1109/IFOST.2011.6021216.
- [27] S. Singh, S. K. Maakar, and S. Kumar, "25 A performance analysis of DES and RSA cryptography," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 2, no. 3, pp. 418–423, May-Jun. 2013.
- [28] M. L. Manna, L. Treccozzi, P. Perazzo, S. Saponara, and G. Dini, "Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update," *Sensors*, vol. 21, no. 2, p. 515, Jan. 2021, doi: 10.3390/s21020515.

## BIOGRAPHIES OF AUTHORS







**Mustafa Noori Rashid**     awarded the Bachelor of Computer science from University of Baghdad in September 2004. He received his Master's degree Faculty of Computer Science and Information Technology from University Putra Malaysia (UPM) in July 2018. Currently, he is the assistant lecturer in the Department of Computer Systems, Technical Institute of Anbar, Middle Technical University, Iraq. His research interests include cloud security, computer networks, distributed computing, and artificial intelligence. He can be contacted at email: mustafan@mtu.edu.iq.



**Leith Hamid Abed**     achieved a BSc (2009), an MSc (2012) in Computer Science from the University of Anbar, Iraq. He received PhD (2019) in Cybersecurity from the School of Computing, Electronics, and Mathematics at the University of Plymouth in Plymouth, UK. His research interests reside in cybersecurity, bio-cryptography, malware analysis and detection, and security management using self-data destruction, and secret sharing. He can be contacted at email: laithhamed@mtu.edu.iq.



**Waleed Kareem Awad**     obtained a bachelor of Computer science in 2009-2010 from the University of Anbar, Iraq. He received M.Sc. communication and network security in 2013-2014, from Anbar University. His research interests are security, cloud computing, multimedia, databases, AI, and image processing. He can be contacted at email: waleed.kareem@uoanbar.edu.iq.