# ITC571 – Final Report Cover Page

| | |
|---|---|
| Full Name | Phanikalyan Palatla |
| Student ID | 11710403 |
| Subject | ITC571 – Emerging Technology and Innovations |
| Assignment Item 4 | Final Report and Seminar Presentation – 45% |
| Due Date | 30 May 2021 |
| Title of the Research | **Blockchain in data and information in cloud security by using cryptography methods** |
| Course Specialisation | Cloud computing/computer networking |
| Blog Address | https://thinkspace.csu.edu.au/phanikalyan/2021/03/12/11710403/ |


.

# Blockchain in data and information in cloud security by using cryptography methods (May 2021)

**Phanikalyan Palatla,11710403 (Cloud computing and computer networking)**

**Cryptography data methods improve cloud data security by using cipher blockchain mode in cryptography improves cloud security and eliminates data breaches. This report analysis symmetric and asymmetric methodologies and provides a detailed discussion on two symmetric and asymmetric methodologies and guidance for a new proposal encryption method for data encryption for cloud security. In this report, current data encryption methods were detailed investigates on each symmetric and asymmetric encryption and Finding new hybrid encryption for all use cases and reduces risks and vulnerabilities from cyberattack issues. The Aim of research compare and contrast the present data encryption methods and critically analyses the methodologies and providing optimum hybrid encryption model will provide all solution for cyberattacks and nullifies any data breaches in the cloud security**

***Index Terms*— Cryptography methods, Cipher blockchain, Symmetric encryption methods, Asymmetric encryption methods, cyberattacks.**

## I INTRODUCTION

Cloud computing was the most common platform used by many organizations to provide better flexibility to the customer. Cloud computing offers the best features like the shared responsibility model to many organizations.[1]. Cloud security handling when data transfers between customers and organization was most challenging to protect from any kind of cyber-attack. In my research provide an optimum solution by implantation of cipher block method eliminates most security concerns.[2].

Cloud offers a shared responsibility model for three deployment models. [3]. Every deployment has responsible some responsibility for the customer and provider. In PASS user is responsible for managing security applications, Workload, and data while the cloud provider was responsible for security for the platform. IASS model offers to User has responsibility for the Application and data while the provider manages hypervisor and VM security. SASS model offers users had responsible for data handling. [1] Users not following encryption techniques when migrates have more likelihood changes to the attacker to interrupt the session. Security has the most concern in the cloud for every client and provider to protect from information security issues. User has more conscious of security on their device implementing, strong firewall and encryption techniques when migrating data to the cloud. [3]

### Overview of cloud security

Lack of proper security standards cause attackers to stole customer sensitive data from data base in figure-1 and how to prevent this malicious activity in figure-2.

In the Figure-1 attackers has two possible way to stole user confidentiality data as indicated with red colour. Hackers tries to access the internet to windows server to gain access to SQL database. Another possible to hacker tries to interrupt the customer database and stole the information tries misuse the information for illegal activities to stop these control measures provide in each step as shown in the figure-2.

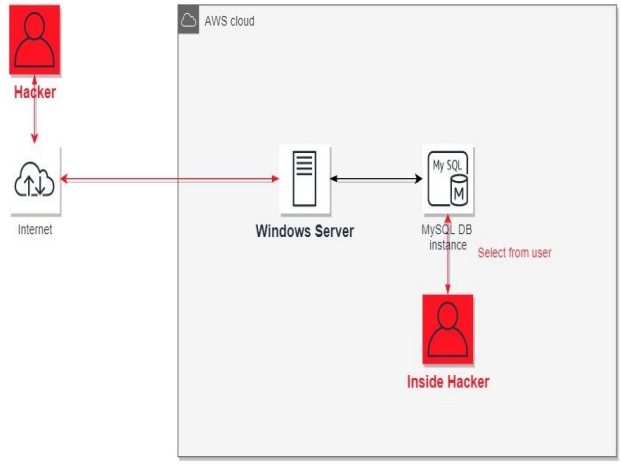


**Figure-1 Attacker tries to intrude SQL server**

Installing proper secure methods in each step can reduces malicious attacks. Hackers and user access to internet resources by installing web application firewall restrict and filters the unauthorized user to the website. DDOS installed along with web application firewall protecting in WAF blocking malicious activity. Biometric access management governance, audit and monitoring users done in Identify access management. Monitoring continuous policy check certification audit checking SQL instance, window server to prevent attacks and also protect public cloud from any malicious attacks. Data protection any deployment model can be retrieved from Encryption methods like symmetric &asymmetric we discuss more detail in paper. security operation running helps monitoring user's activity in the cloud so this malicious threats and vulnerabilities.

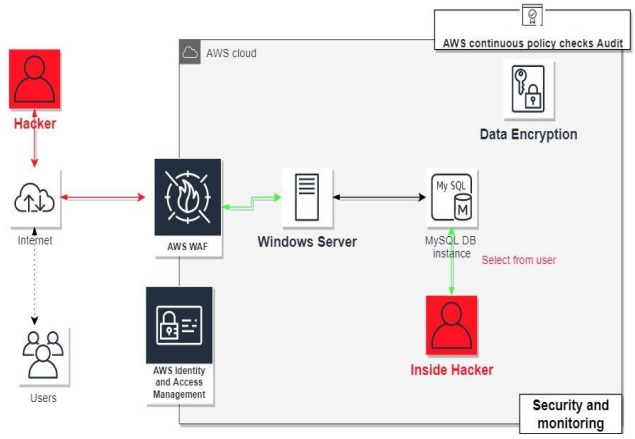


**Figure-2 Overview diagram of cloud security**

**Implementation of cipher blockchain mode in cryptography:** cipher blockchain mode forms number of data block and there interconnected to each other. Cipher blockchain helps to improves more secure way to cryptography methods.[2] . Cipher blockchain mode used in all models in the report use same concept of blockchain the data information divide in to number of blocks each block connected at end to form a meaningful plain text.[4]

This paper is organized as follows: Section 2 demonstrates a Data protection encryption and uses techniques with the detailed discussion of algorithms used. Data techniques symmetric encryption methods DES, AES and asymmetric methods RSA algorithms methods were discussed in section2 Section 3 shows plots of different encryption methods and key findings from plots were detailed obtained as result of data prediction and conclusion can be drawn. Section 4 discusses the experiment results in detail with any issues faced and optimism solution for the issues and purposed new hybrid model. Section 5 conclusion and Future work of my research was discussed.

## II METHODS and Materials

In this report comparison of time for symmetric and asymmetric in anaconda power script for input was demonstrated in the result section. In this research, the most common asymmetric algorithm was chosen, and for symmetric AES and DES comparison taken place in anaconda script to purpose a solution for Data protection in the cloud.[5]

**Cryptography methods** were used in data protection in the cloud to secure data to the database using the cipher block method for all cryptography in this paper.

**Asymmetric method RSA**

The asymmetric method has different keys for receiver and sender for data migration between one sender to another sender.[6]**.** In the RSA algorithm sender has one key and ciphertext to send to a receiver and the receiver has its own generated key and decrypts the message (ciphertext sends from sender) with help private key from the receiver decodes the ciphertext to plain text.[5]. RSA was the most common asymmetric used. [7].

a) **Generation of key: -** Randomly selecting two large prime numbers such that there, not co-primes. P1 and P2 are two positive prime numbers E is the encryption key for the sender to encrypt to ciphertext and D is the decryption key for receiver along with ciphertext send by sender must follow these conditions listed in the Table.[6]

| Keys | Explanation | Satisfy condition |
|---|---|---|
| P1,P2 | Large positive prime numbers. Here is function two inputs. | N =P1*P2<br>Ψ(N)=(P1-1)*(P2-1) |
| E | *Used for encryption key E is large positive numbers* | *1<E<* Ψ(N).<br>*GCD(E,* Ψ(N))=1 |
| *D* | *Used for Decryption key D is large positive numbers.* | *E*DMod(*Ψ(N))=1 |

**Table 1 Keys representation and satisfy condition.**

b) **Encryption mechanism:-** To perform the encryption mechanism sender has a key for encryption (E, N)and

plaintext to convert to ciphertext. Output sending the ciphertext to the receiver. The sender has to follow these conditions listed in the Table.[6]

| Action for key | Description | condition |
|---|---|---|
| Input to sender | M,N,E<br>M = encrypt to plain text. | 1:C=M^E mod(N);<br>c= cipher text |
| Output to receiver | M ,N,C | 1:C=M^E mod(N) |

**Table 2 Keys representation and satisfy condition**

**c) Decryption Mechanisms: - :-** To perform decryption mechanism receiver has a key for encryption (D, N)and encrypts ciphertext from the sender. Output Ciphertext to plain text. The receiver has to follow these conditions listed in the Table.[6]

| Action for key | Description | condition |
|---|---|---|
| Output from receiver | C,N | 1:C=M^E mod(N);<br>c= cipher text |
| input from sender | C,N,D ; M=cipher text from sender | 1:M=C^D mod(N) |

**Table 3 Keys representation and satisfy condition.**

**symmetric method: -** Symmetric Encryption has only one key for both user and receiver. The user must send the key to the receiver confidentially. This symmetric method discussing more detail on DES and AES encryption methodology. [5].

1. **DES encryption method:** In this encryption process handles up to 64-bit plain text.[8]. DES operates show set of calculations in the round and repeats the entire cycle 16 times.[9]. Generally, In DES encryption 64-bit plain text was divide into two parts LHB and RHB.[10]. DES encryption involves an iteration process for more than 16 and finally, the two parts combine XOR calculation. Some steps to consider with both LHB is L0 and R0

- Li=Ri-1
- Ri=Li-1 XOR F(Ri-1, Ki)

After some key transposition and round 16 to get the final text and key. DES involves two stages at encryption and decryption.

1. **Encryption mechanism: -** To perform the encryption mechanism sender has a key for encryption key and plaintext to convert to ciphertext. Output sending the ciphertext to the receiver. In this user initiates DES mode of operation for 16 rounds
2. **Decryption Mechanisms: -:-** To perform the decryption mechanism receiver has a key for decryption send by the user and cipher output at end of 16 stages and the sender to decrypt the cipher message to plaintext.[10]

1. **AES encryption method: -** In this encryption model handles up to 128 bytes of plain text.[11]. AES encryption models have rounds of stages n=10,12,14 depending on key length. AES represents plaintext in matrix form and key in matrix form and performs four operations as shown below.[12]

- **Byte substitution mechanism ( S-box calculation**):- In this mechanism performs a non-linear type of operation and a combination of logic. In this type of plain text convert the plain text to S-box in the table in the matrix
- **. Row shifting transposition:** In the step entire matrix perform 3 step calculation. Shifting of Row in matrix implies First remain unchanged, second Row shift to one left, Third-row shifts to two left and final row shifts three to left.
- **Shifting column transposition:** The conversion of the column to Hexadecimal conversion and multiply of constant number at every column and nonlinear computation takes place in this stage.
- **Round Key transposition:** In this step, each column undergoes XOR calculation with KEY values and the same procedure to all columns applies the same mechanism.[12].

**a) Encryption mechanism: -** To perform the encryption mechanism sender has a key for the encryption key and plaintext to convert to ciphertext. Output sending the ciphertext to the receiver. In this user initiates AES mode of operation for 10,12,14rounds. Sends ciphertext to the user.

**b) Decryption Mechanisms: -** To perform decryption mechanism receiver has a key for decryption send by the user and cipher output at end of 10,12,14 stage and sender to decrypt the cipher message to plaintext with help of key provider by the sender.

## III RESULTS

In this comparison of three algorithm and results of time encryption time and key compared by using anaconda script.

First creating menu bar of three algorithms methods as shown in the figure and compare option for Between three algorithm made some assumptions.

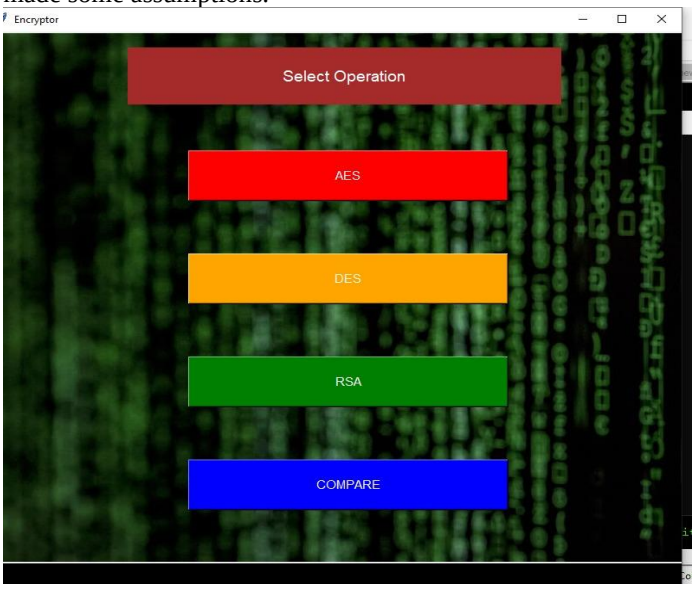

**Figure-3 Menu creation for execution different operations.**

After clicking mode of operation DES, RSA, AES for example AES mode list of menus like to whether to encrypt or decryption option. In encryption option ask for text to encrypt where user can enter text to encrypt the function and key was automatic generated by each function which was define in the function in anaconda script. In decrypt ask for encrypted file and key store in the user with the help of option decrypt the message.

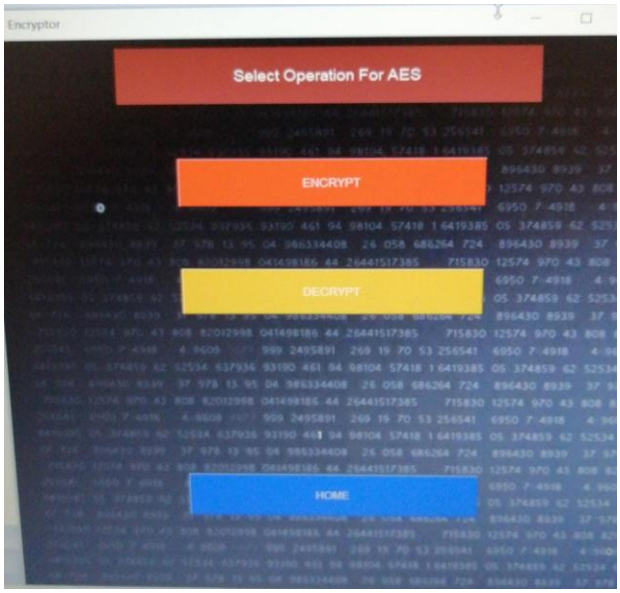


**Figure-4 Mode of operation for execution different operations.**

**In this Results section we will compare encrypt time and decrypted time and key generated by anaconda script.**

**Comparison of all three algorithm for small input (10-20) words.**

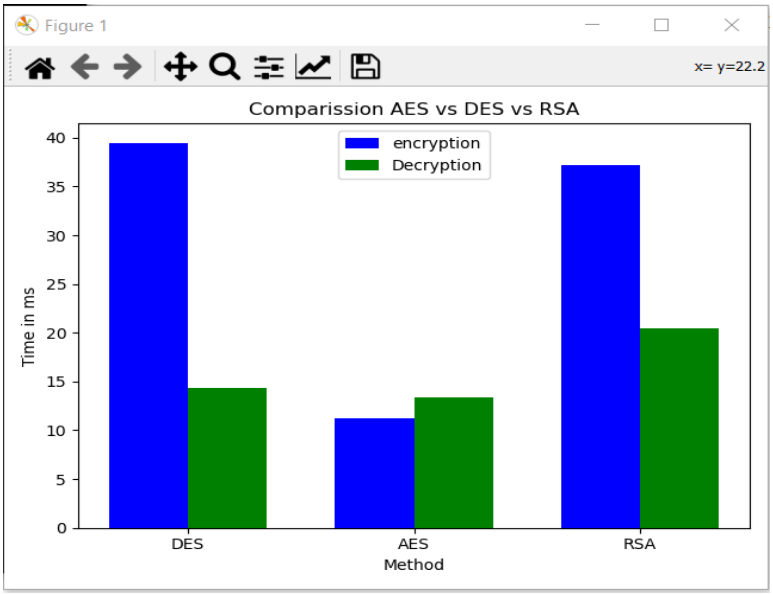


**Figure-5 Comparison between AESvsDESvsRSA**

For small inputs time take for all three methods is similar we can use any type of encryption based on need of the situation.

| Type of methods | Key used for encryption | Time taken for encryption | Time taken for decryption |
|---|---|---|---|
| DES | Same key used for Encryption and decryption | 39ms | 14mS |
| AES | Same key used for Encryption and decryption | 11mS | 13mS |
| RSA | E-encryption D-decryption N-satisfy number | 38mS | 20mS |

**Table -4– output description for small inputs**

All three Encryption AES less time than DES and RSA as shown in the table

**Comparison of all three algorithm for larger input (>200)words.**

Same like comparison large text in my case I just took 284 words general paragraph and compare all three methods symmetric analysis and asymmetric

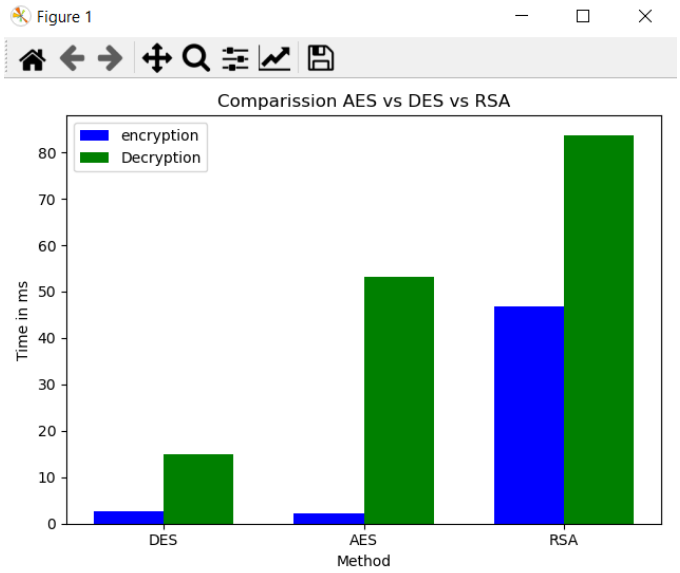


**Figure-6 Comparison between AESvsDESvsRSA**

| Type of methods | Key used for encryption | Time taken for encryption | Time taken for decryption |
|---|---|---|---|
| **DES** | **Same key used for Encryption and decryption** | **26ms** | **14mS** |
| **AES** | **Same key used for Encryption and decryption** | **23ms** | **53mS** |
| **RSA** | **E-encryption D-decryption N-satisfy number** | **46ms** | **83mS** |

**Table-5 – output description for large inputs**

From the output we can clearly say time take decryption in the RSA algorithm is more than the other two methods as shown in the figure. AES and DES have similar times and less than the RSA algorithm. AES and DES have almost the same time as the RSA algorithm.

**DISCUSSION**

In this research analysis all three methods symmetric and asymmetric methodology to purpose a solution for data migration to the cloud for all organizations. In both cases for large input and smaller inputs time take for the symmetric algorithm (DES, AES) is less than the RSA algorithm. Data Encryption asymmetric methodology (RSA) algorithms more code complex and more costly than other symmetric methods.

**From the result, these are conclusion drawn**

- Comparison between Symmetric (AES, DES) and Asymmetric (RSA) and based on result RSA algorithm most secure Cryptography method due to different key used in encryption and decryption and more complex in key generation.
- While AES, DES uses the same key for encryption and decryption but the time taken for the encryption method is less than the RSA algorithm.

Depending on the organization like small organizations cannot afford the RSA cost of implementation more they comprise and using the low encryption methodology may like to have cyber-attacks. Medium organization can afford all type of methods so like the hood of risks were less than small organization.

**Proposing solution for these types of issues:**

Proposing an Automated hybrid encryption technique in data migration from one place to another place. The automated hybrid model comprises Asymmetric and symmetric encryption techniques based on the migration this can be implemented as per usage charge to the organization.[3]. For instance, organization A wants to migrate to the cloud involves stage choose a cloud provider, purchase cloud provider, Data phase, the Application phase, Implantation on their services on their organization and finally test services.[13]

Migrating resources involves so many stages like data case-sensitive information use Asymmetric model and rest of the phase use symmetric encryption this reduce cost on data security and also reduces cyber-attacks. Automated hybrid data encryption model has both asymmetric and symmetric operation like transforming sensitive information usage of Asymmetric and rest other symmetric this improve security and improves business to any organization.[14].

**Future work**

Analyze Automated hybrid encryption model detailed analysis and work on automated hybrid encryption model. In future analysis benefits and comparison different encryption methodologies. Building prototype for automated hybrid encryption model and then working model for automated hybrid and clearly describes its use case and how to implement in the cloud security to avoid from cyber-attacks.

**CONCLUSION**

It can be concluded that provided most efficient techniques in data encryption methodologies improves cloud security and eliminates data breaches and cyber-attacks. Data security by implanting cipher Block Methods in symmetric and asymmetric encryption were analyzed in my research. Cloud data security was analyzed and a comparison between symmetric and Asymmetric was analyzed in this report. The finding demonstrated a comparison between symmetric and asymmetric data encryption and key conclusion drawn from these methods in my report. Symmetric encryption methods

proved that take less time for encryption whereas Asymmetric strong method encryption but there is code complexity and more cost compared to symmetric encryption. [15] **.**Thus, the existing system asymmetric encryption is generally used for higher business due to maintaining cost more than symmetric while symmetric not complete assure from data breaches and cyber-attacks. Solution for these issues proposing a hybrid automated encryption model consists of symmetric and asymmetric encryption model. These methods help an organization like sensitive information uses asymmetric encryption and all other case uses of symmetric other phases reduce and nullify most of the cyber attacks and this improves business for the organization.

**REFERENCES**

[1] T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," in *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Apr. 2010, pp. 27–33. doi: 10.1109/AINA.2010.187.
[2] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A Survey on Blockchain for Information Systems Management and Security," *Inf. Process. Manag.*, vol. 58, no. 1, p. 102397, Jan. 2021, doi: 10.1016/j.ipm.2020.102397.
[3] S. Sarmah, "Cloud Migration-Risks and Solutions," pp. 7–11, Jun. 2019, doi: 10.5923/j.scit.20190901.02.
[4] M. Mayuranathan, M. Murugan, and V. Dhanakoti, "Enhanced security in cloud applications using emerging blockchain security algorithm," *J. Ambient Intell. Humaniz. Comput.*, Jul. 2020, doi: 10.1007/s12652-020-02339-7.
[5] "Full article: Review of Cryptography and Network Security: Principles and Practice, Fifth Edition." https://www-tandfonline-com.ezproxy.csu.edu.au/doi/full/10.1080/01611194.2010.533253 (accessed Mar. 17, 2021).
[6] "Fast and Area Efficient Implementation of RSA Algorithm," *Procedia Comput. Sci.*, vol. 165, pp. 525–531, Jan. 2019, doi: 10.1016/j.procs.2020.01.024.
[7] R. Shams, F. Khan, and M. Umair, "Cryptosystem An Implementation of RSA Using Verilog," *Int. J. Comput. Netw. Commun. Secur.*, vol. 1, pp. 102–109, Aug. 2013.
[8] P. Patil, P. Narayankar, Narayan D.G., and Meena S.M., "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, 2016, doi: 10.1016/j.procs.2016.02.108.
[9] Y. Wu and X. Dai, "Encryption of accounting data using DES algorithm in computing environment," *J. Intell. Fuzzy Syst.*, pp. 1–11, 2020, doi: 10.3233/JIFS-179994.
[10] M. A. Seif Eldeen, A. A. Elkouny, and S. Elramly, "DES algorithm security fortification using Elliptic Curve Cryptography," in *2015 Tenth International Conference on Computer Engineering Systems (ICCES)*, Dec. 2015, pp. 335–340. doi: 10.1109/ICCES.2015.7393071.
[11] J. Daemen, *The Design of Rijndael The Advanced Encryption Standard (AES)*, 2nd ed. 2020. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020. doi: 10.1007/978-3-662-60769-5.
[12] R. R. Farashahi, B. Rashidi, and S. M. Sayedi, "FPGA based fast and high-throughput 2-slow retiming 128-bit AES encryption algorithm," *Microelectron. J.*, vol. 45, no. 8, pp. 1014–1025, 2014, doi: 10.1016/j.mejo.2014.05.004.
[13] D. G. Rosado, R. Gómez, D. Mellado, and E. Fernandez-Medina, "Security Analysis in the Migration to Cloud Environments," *Future Internet*, vol. 4, no. 2, pp. 469–487, 2012, doi: http://dx.doi.org.ezproxy.csu.edu.au/10.3390/fi4020469.
[14] A. Naseer and H. Zhiqui, "Cloud Computing Security Threats and Attacks with Their Mitigation Techniques," Oct. 2017, pp. 244–251. doi: 10.1109/CyberC.2017.37.
[15] H. Huang, Q. Chen, Y. Zhou, and Z. Huang, "Blockchain-Based Secure Cloud Data Deduplication with Traceability," in *Blockchain and Trustworthy Systems*, Singapore, 2020, pp. 295–302. doi: 10.1007/978-981-15-9213-3_23.