ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

A CLOUD COMPUTING PLATFORM-BASED ANALYSIS OF DATA LEAKAGE DETECTION IN CREDIT CARD TRANSACTIONS

K.C. Chandra Sekaran
Associate Professor, Department of Computer Science, Alagappa Govt. Arts College, Karaikudi, Tamilnadu, India
chandrasekarankc@agacollege.in

ABSTRACT

Data leakage is a significant problem in data science and machine learning because it can result in models that are overly accurate but perform poorly when faced with real-world decision-making situations. The concept of data leakage is examined in this course, with a focus on two specific types—leaked predictors and leaked validation procedures. The credit card transaction data used as the basis for the example dataset was examined using econometric methods. Investigating the effects of data leakage in the context of financial data can be started out with great success with this dataset. This study endeavor emphasizes the need of comprehending leakage and its potential consequences. Leaky predictors are used when features that shouldn't be present during model training but are present during prediction unintentionally add data that could lead to overfitting. The use of wrong validation methods, on the other hand, exposes the model to data it shouldn't have access to, inflates performance metrics, and eventually leads to poor generalization. As a solution to these issues, cloud computing techniques are recommended. A scalable and secure environment for data management, processing, and model training is provided via cloud computing. Data scientists can effectively separate training data from validation data using cloud platforms, ensuring that data leakage is kept to a minimum. In this research work the various encryption algorithms in cloud computing include Data Encryption Standard (DES), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) and BLOWFISH to analyse the speedup, meantime and buffer time using the different credit card datasets and identify the best method based on the performance metrics.

Keywords: Leaky Validation Strategies, Leaky Predictor, Cloud Computing, RSA, AES, DES, BLOWFISH.

1. INTRODUCTION

Cloud computing (CC) has transformed the way businesses handle and store data by allowing them to access scalable and cost-effective computer resources over the internet. With this ease, however, comes the problem of guaranteeing the security and safety of sensitive information, such as credit card data. Credit card leakage protection in cloud computing is an important aspect of protecting financial and personal information. It consists of a set of practises, technologies, and policies designed to prevent unauthorised access, theft, or exposure of credit card information within cloud-based environments. The distribution of computing services such as storage, processing power, and applications via the internet is referred to as cloud computing. Cloud service providers (CSPs) such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) generally provide these services. Credit card information, personally identifiable information (PII), and other sensitive data is stored in the cloud by organisations. Because of the possibility for financial benefit, credit card data is especially appealing to cybercriminals.

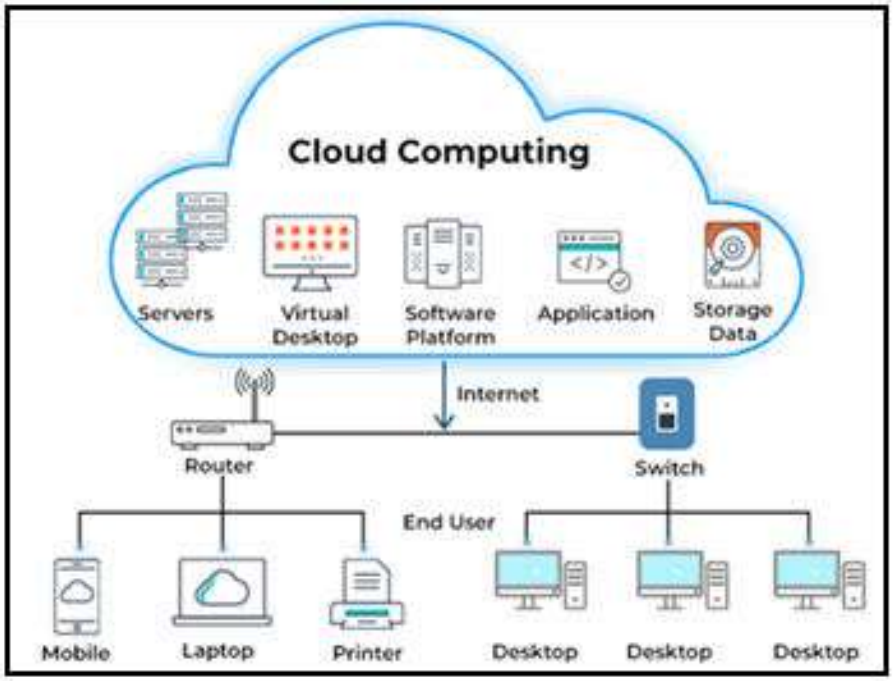

Figure 1: Architecture of Cloud Computing

Figure 1 shows that the distributed computing becomes more visible in today's digitalized world, cloud-based networking architecture must be transparent in its design. Cloud computing engineering accurately compares to many segments that make up the overall framework structure in this manner. The cloud networking components connect to platforms such as Front-End, Back-End, and cloud-based delivery. On the consumer side, the front-end is more like cloud computing. This section discusses the interfaces, applications, and organisational structures that enable the availability of a cloud architecture. However, this does not imply that all registration frameworks will behave as a single interface. A cloud networking architect is in charge of creating and executing cloud networking solutions for these.

Credit card leakage is the unintentional disclosure or unauthorised access to credit card information. This can happen as a result of data breaches, misconfigured cloud services, insider threats, or other cloud-related risks. Several strategies are used to defend against credit card leaks in cloud computing. To prevent unauthorised access, data should be encrypted both in transit and at rest. To restrict access to credit card data, implement robust access control regulations and role-based access control (RBAC). Tokenization is the process of replacing sensitive credit card data with tokens, which reduces the risk of storing actual card information. Firewalls and Intrusion Detection are used to monitor and filter network traffic for potential threats using firewalls and intrusion detection systems. Continuous monitoring and auditing are used in security monitoring to discover and respond to questionable actions. Compliance Standards adheres to industry-specific compliance standards such as PCI DSS (Payment Card Industry Data Security Standard) for credit card data handling. In an increasingly digital environment, credit card leakage protection in cloud computing is a critical part of preserving data security and compliance. To limit risks and retain customer trust, organisations must take a proactive and multi-layered strategy to safeguarding credit card data and other sensitive information within their cloud systems.

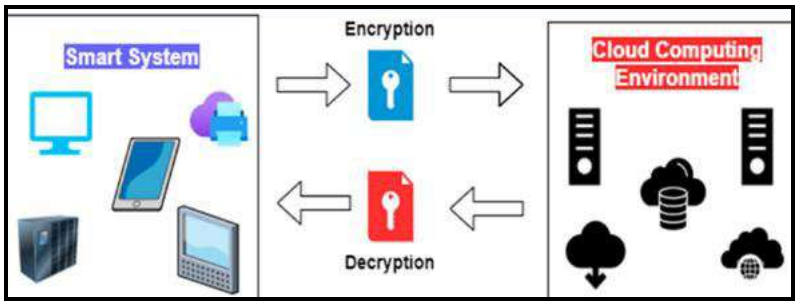

Figure 2: Encryption method in cloud computing environment

Figure 2 shows that the databases are widely used in cloud computing systems. Database encryption is used to safeguard the information held in databases. Encrypting entire databases, individual tables, or columns containing sensitive information is one example. Encryption is critical in cloud computing environments for protecting data from unauthorised access and maintaining data privacy and security. It should be part of a broader cloud security plan that includes access control, key management, and adherence to applicable rules and industry standards.

2. REVIEW OF LITERATURE

A literature review is an essential component of academic research that benefits both researchers and the research process as a whole. Researchers can find areas for additional research by reviewing existing material. It sets the stage for the investigation by summarising previous studies, theories, and conclusions on the subject. This assists researchers in situating their work within a larger academic and intellectual perspective. A research work carried out by Roychowdhury et al. in [1], in which that the e-health care dataset in cloud were used in this research work to identify and prevent the threats and attacks of the chosen dataset. The encryption, watermarking and proposed hybrid methods are used in this research work to prevent the cloud-based health care dataset more efficiently.

Another research paper titled as" Review on Prevention of Data Leakage in Cloud Server by Utilizing Watermarking and Double Encryption Techniques" in [2], the data breaches are common in real-world cloud storage systems, making secure data transmission and copyright protection of multimedia information challenging. The use of digital watermarking has been offered as a solution to the problem of copyright protection. To secure the data and prevent unauthorised access, encryption techniques are also used. To efficiently exchange multimedia files, proposes combining both watermarking and proxy re-encryption techniques. The research paper done by Devi, B et al. in [3], in which that the increased use of numerous systems, services, and applications, exchanging multimedia data has become an important part of people's daily lives. Data leakage, on the other hand, is a common issue in cloud storage systems. To enable secure multimedia material sharing, the recommended solution combines watermarking and Proxy Re- (PRE). Encryption techniques are also employed to prevent unauthorised access to data. The suggested method encrypts a secret key using a specific key, then combines it with encrypted key data before embedding it in an image using the Least Significant Bit (LSB) technique. After inserting the sensitive information, the image can be encrypted using the ECC Encryption technique.Built-in data to the verification mechanism allows authenticated individuals to recover the decryption key, allowing unauthorised access to be identified and content redistribution to be restricted. The proposed application has the potential to prevent unauthorised cloud access and assure the security of multimedia data exchange.

A research paper titled as "Data Leakage Discovery in Cloud Using Watermark Fashion" in [4], There is a strong demand to keep the services stable and safe, which is based on the growing number of drug users. When a customer spills sensitive information, the specific customer responsible for the breach should be identified as quickly as possible. As a result, the data travelling from the distributor to the agents must be monitored. A data leakage detection system based on watermarking is suggested. This system investigates data tampering and concludes that one or more agents are to blame for the data leak. Furthermore, the procedure is afterwards utilised on design palettes. Another research paper is carried out by Alshutayri, Areej in [5], in which that the necessity of

accurately forecasting fraud episodes through payment procedures, this study evaluated the credit card payment methods used for movie tickets, analysing and predicting such incidents using the machine learning logistic regression method. This study examined a dataset of 284,807 cinema ticket credit card transactions made by European cardholders on two days in September 2013, including 492 fraudulent purchases. The proposed method's results demonstrated a prediction accuracy of 99%, demonstrating its outstanding prediction ability.

3. MATERIALS AND METHODS

Storage security and data security are required to store, manage, share, analyse, and use the large quantity of data stored in the cloud. The data should be secure, authenticated, and encrypted so that three levels of security may be supplied. To gain access to a cloud-based online application that would attempt to alleviate the problem of data privacy segmentation. We investigated many encryption algorithms such as AES, DES, and Blowfish to assure data security in cloud computing. This research work evaluating and comparing various encryption algorithms, such as DES, AES, RSA, and Blowfish, with the goal of determining their performance in terms of speedup, meantime, and buffer size when applied to credit card datasets of various sizes (15MB, 18MB, 58MB, and 72MB). The goal is to figure out which encryption method is best for protecting credit card information in a cloud computing or data storage environment. The encryption techniques to be examined include DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and Blowfish. These algorithms combine symmetric and asymmetric encryption methods. To mimic real-world settings and evaluate the scalability and performance of the encryption algorithms, four separate credit card datasets of diverse sizes (15MB, 18MB, 58MB, and 72MB) are chosen.

This study's performance measures evaluate the following performance metrics for each encryption algorithm.

- Speedup- The improvement in performance produced by applying parallel processing or optimised methods over a reference (e.g., unencrypted data) is measured as speedup.
- Meantime is the average time it takes to encrypt or decode a dataset.
- Buffer Size- The amount of memory or storage space necessary to process encrypted data efficiently is referred to as buffer size.

Advanced Encryption Standard (AES): The Advanced Encryption Standard (AES) is a commonly used encryption technique that is critical in guaranteeing data security and secrecy in cloud computing environments. The storage, processing, and retrieval of data and applications over the internet, frequently by third-party service providers, is referred to as cloud computing. Encryption is used to safeguard sensitive data from unauthorised access or breaches during transmission and storage on the cloud, and AES is a popular encryption method due to its durability and effectiveness. AES employs symmetric key cryptography, which means it use the same key for both encryption and decryption. This makes it appropriate for cloud computing, where data must be encrypted before storage or transmission and decrypted when accessed. AES uses fixed-size data blocks, typically 128 bits, and different key lengths, such as 128, 192, or 256 bits, depending on the amount of security desired.

The Data Encryption Standard (DES)*:* is a symmetric-key encryption technique that was once widely employed for data security. While it was thought to be robust in its early days, developments in computing power have rendered it vulnerable to brute force attacks. DES is a symmetric-key encryption technique that employs a fixed encryption key of 56 bits. It encrypts and decrypts data in 64-bit chunks since it operates on 64-bit data blocks. DES employs a Feistel network structure, in which data is split in half and subjected to many rounds of substitution and permutation.

RSA (Rivest-Shamir-Adleman): It is a popular asymmetric key encryption method that is critical for data security in cloud computing environments. Asymmetric key encryption, commonly known as public-key encryption, uses two keys: one for encryption and one for decryption. Each entity (for example, a user or a cloud server) in RSA generates a pair of keys—a public key and a private key. The public key is distributed to others, while the private key is kept private. The mathematical difficulty of factoring big semiprime integers, which is computationally

infeasible for sufficiently large numbers, underpins the security of RSA. When a user wishes to transfer data to the cloud or another user, they encrypt the data with the recipient's public key. This ensures that the data can only be decrypted and accessed by the receiver who has the associated private key. In secure communications between clients and cloud servers, RSA encryption is extensively utilised. RSA can also be used to generate digital signatures, which aid in data integrity and cloud authentication. A user can use their private key to sign a piece of data, and anyone with access to the associated public key can verify that the material has not been tampered with. RSA is a widely established and secure encryption method used in a variety of cloud computing applications, including data security in transit and at rest, as well as secure authentication and key exchange procedures. Proper deployment and key management are critical for guaranteeing cloud data security.

Blowfish: Blowfish symmetric-key block cypher encryption technique in 1993. While it is well-known for its speed and security, it is crucial to note that Blowfish is currently considered relatively antiquated in terms of cryptographic strength when compared to more modern options such as AES (Advanced Encryption Standard). Blowfish is a symmetric-key encryption method, which means it uses the same key for encryption and decryption. Symmetric-key encryption is frequently used in cloud computing to secure data at rest (stored data) and data in transit (during communication). Blowfish was previously a popular encryption technique due to its speed and security; however, it is no longer regarded as a best practise for securing data in cloud computing, owing to the availability of more resilient and current encryption algorithms such as AES. To maintain data security, organisations should prioritise effective key management practises and employ robust and up-to-date encryption techniques to protect data in the cloud.

4. Performance Analysis of Encryption Algorithm

Table 1 shows that the rows correspond to various dataset sizes ranging from 15 KB to 72 KB. The values in each table cell represent the time (or some other performance metric) required by the related encryption technique to encrypt the dataset of that size. It appears to be a performance comparison of different encryption algorithms in terms of how efficiently and rapidly they can encrypt credit card databases of various quantities, both locally and in the cloud.

Table 1: Mean Processing Time on a Local System and a Cloud Network

Input	AES	AES Cloud	DES	DES Cloud	BLOWFISH	BLOEFISH cloud
15 KB	13.5	3.5	9.5	4	6	4
18 KB	15.7	3	11	3.5	5.7	3
58 KB	22	4	4.16	7.5	9.26	3.76
72 KB	25.6	4.76	50.35	9.98	16.7	4

AES processing times on a local machine range from 13.5 ms for a 15 KB dataset to 25.6 ms for a 72 KB dataset. Processing times in a cloud network range from 3.5 ms for a 15 KB dataset to 4.76 ms for a 72 KB dataset. DES processing times on a local system range from 9.5 ms for a 15 KB dataset to 50.35 ms for a 72 KB dataset. Processing times in a cloud network range from 4 ms for a 15 KB dataset to 9.98 ms for a 72 KB dataset. Blowfish processing times on a local system range from 6 ms for a 15 KB dataset to 16.7 ms for a 72 KB dataset. Blowfish processing times in a cloud network range from 3 ms for a 15 KB dataset to 4 ms for a 72 KB dataset.

Processing times for all three encryption algorithms (AES, DES, and Blowfish) are generally faster in a cloud network than on a local device. This could be attributed to the cloud network's scalability and optimised hardware. AES has the longest processing durations, followed by DES and finally Blowfish. This is consistent with the belief that AES is a more computationally costly algorithm that provides strong security.

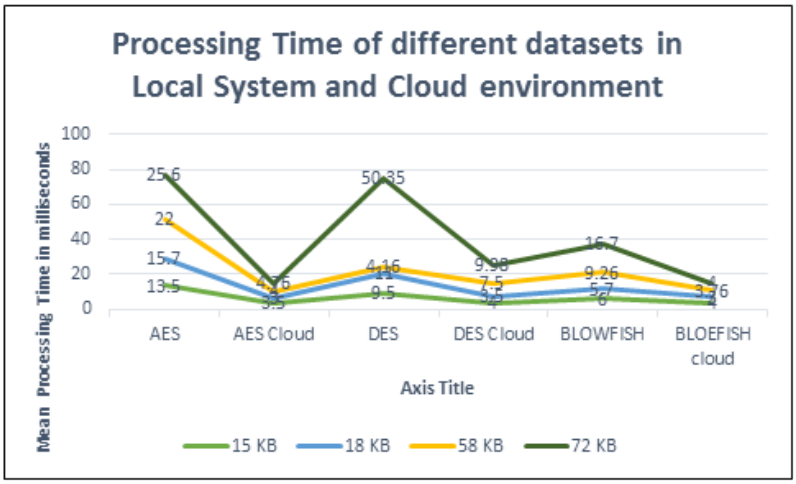

Figure 3: Graphical representation of Comparison of Processing Time on a Local System and a Cloud Network

Figure 3 shows the processing times rise as the dataset size increases, as larger datasets take longer to encrypt. If speed is important, Blowfish may be a suitable solution, especially when running in a cloud network, because it regularly has shorter processing times than AES and DES. However, security concerns must also be addressed. Because of its shorter key length, AES is typically regarded as a highly secure encryption technique, whereas DES is seen as less secure.

Table 2: Local system mean time algorithm comparison with diverse input just cloud environment

Input	AES Cloud	DES Cloud	BLOEFISH cloud
15 KB	3.5	4	4
18 KB	3	3.5	3
58 KB	4	7.5	3.76
72 KB	4.76	9.98	4

DES has the longest processing times among the three encryption algorithms in a cloud setting, followed by AES and then Blowfish. When performed in the cloud, Blowfish consistently has lower processing times across different dataset sizes. This shows that, in this case, Blowfish is the fastest of the three options. While AES and DES are well-known for their high levels of security, Blowfish is a comparatively quick encryption technique. The decision between these three methods is determined by the application's specific requirements. Blowfish may be a good solution if speed is important in a cloud environment and security needs can be addressed.

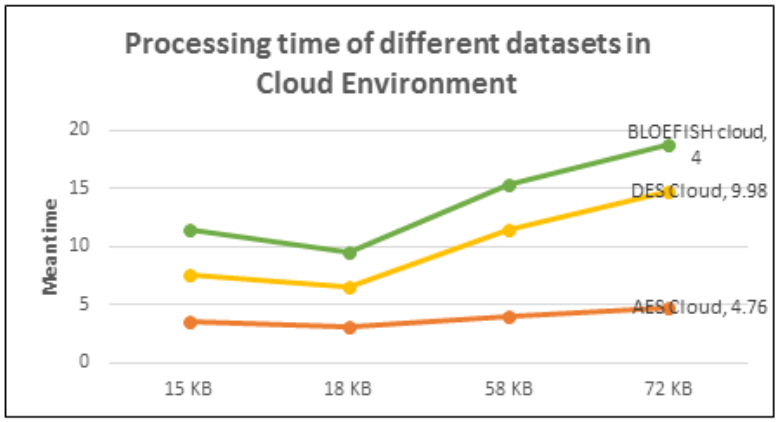

Figure 4: Processing time of different datasets in Cloud Environment

The processing times for all three techniques rise as the dataset size increases, which is to be expected because larger datasets take longer to encrypt. The relative performance order of the algorithms, on the other hand, remains consistent.

Table 3: Speed up ratio analysis

Speed up Ratio of the Algorithm			
Input	**AES**	**DES**	**BLOWFISH**
15 KB	8.7	4.73	3
18 KB	8.2	4.98	3.4
58 KB	8	5.2	4.1
72 KB	7.3	5.69	4.8

The speed-up ratio describes how much faster an algorithm operates when compared to a reference point. The reference point in this example could be a baseline scenario or a different algorithm. Higher speed-up ratios show that an algorithm outperforms or outperforms the reference point. AES has the largest speed-up ratio in this situation, followed by DES and then Blowfish. AES consistently achieves the highest speed-up ratios over a wide range of dataset sizes. In terms of processing speed, this shows that AES surpasses the other two methods.

DES and Blowfish also have speed-up ratios larger than one, suggesting that they are quicker than the reference point, but they are slower than AES in general. The speed-up ratios change as the dataset size increases, but the relative performance order of the algorithms remains constant. The fastest is AES, followed by DES and then Blowfish. As seen by increased speed-up ratios, AES appears to be the fastest solution across different dataset sizes.

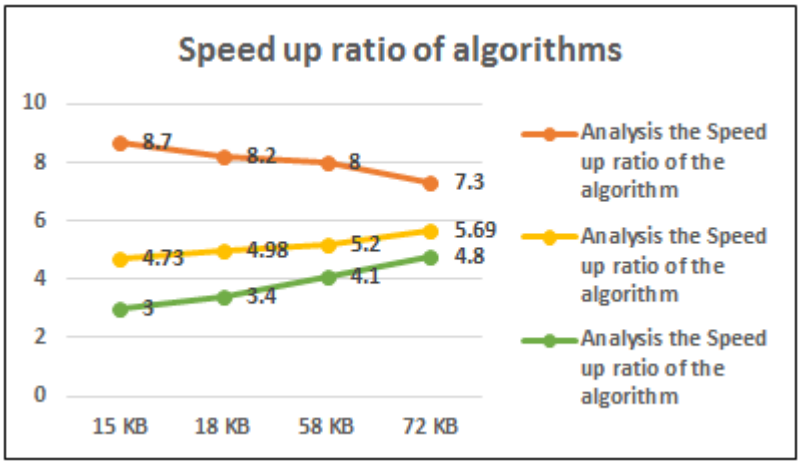

Figure 5: Speed up ratio analysis

Based on this evidence, DES and Blowfish are likewise relatively fast but consistently slower than AES. However, in addition to processing speed, the choice of encryption method should take into account other variables such as security needs, interoperability, and compliance with industry standards.

Table 4: Buffer size analysis

Algorithm	Size	Encryption Time in Sec.	Decryption Time in Sec	Buffer Size
DES	154	3.1	1.2	160
AES		1.7	1.5	162
RSA		7.9	5.3	226

The table 4 displays the encryption and decryption times for three distinct encryption methods with varied buffer sizes (DES, AES, and RSA). When analysing the performance of encryption methods, buffer size is a significant issue to consider. DES has a buffer size of 160 bytes. DES encryption takes 3.1 seconds and decryption takes 1.2 seconds.

AES's buffer size is 162 bytes. AES encryption takes 1.7 seconds and decoding takes 1.5 seconds. RSA's buffer size is 226 bytes. The RSA encryption time is 7.9 seconds, and the decryption time is 5.3 seconds. The size of the buffer has a considerable impact on the performance of certain encryption techniques. In general, larger buffer sizes result in longer encryption and decryption times. RSA has the longest encryption and decryption times due to its enormous buffer size (226 bytes). Encryption and decryption speeds are usually similar, although decryption is slightly faster. This is understandable given that decoding often takes less processing effort than encryption.

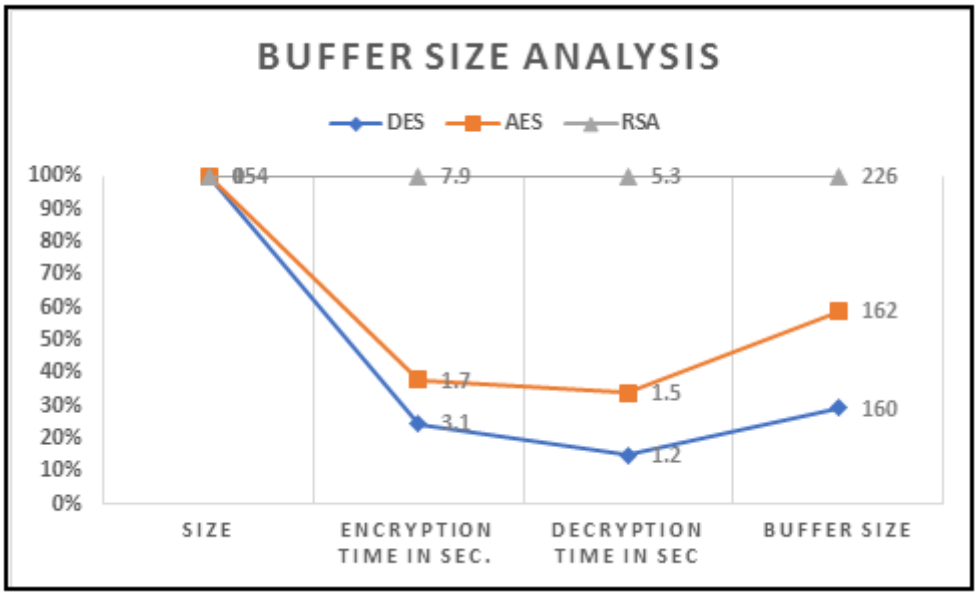

Figure 6: Speed up ratio analysis Graphical representation

Despite having a slightly bigger buffer capacity than DES, AES outperforms DES and RSA in terms of encrypting and decryption times. DES provides the second-best speed performance; however, it is slower than AES. It does, however, provide a trade-off between speed and security. RSA, an asymmetric encryption method, is much slower than both DES and AES. RSA is generally employed for tasks such as key exchange and digital signatures, where security takes precedence above speed.

5. CONCLUSION

Algorithm Performance of AES, RES, and DES In terms of encryption and decryption speed, AES exceeds both DES and RSA. AES is consistently faster than DES, despite having a slightly larger buffer capacity. DES provides a good blend of speed and security and outperforms RSA, but it is slower than AES. Because of the complexity of its mathematical calculations, RSA, an asymmetric encryption technique, is substantially slower than DES and AES. RSA is commonly used for tasks such as key exchange and digital signatures where security is paramount. Buffer size has a considerable impact on the performance of encryption and decryption methods, according to data on encryption and decryption times with varying buffer sizes for three encryption algorithms (DES, AES, and RSA). In general, larger buffer sizes result in longer processing times. AES is the best option. Even with a somewhat higher buffer size, it regularly outperforms the other two algorithms in terms of encrypting and decryption times. AES provides an excellent blend of security and performance and is widely used in a variety of applications.

6. REFERENCES

[1] Roychowdhury, Saptarshi, and Binod Kumar Singh. "A Hybrid and Multi-objective Approach for Data Leak and Tamper Detection in Healthcare Cloud Data." In Machine Vision and Augmented Intelligence: Select Proceedings of MAI 2022, pp. 275-285. Singapore: Springer Nature Singapore, 2023.

[2] P. D. B, D. S, A. N. K and H. Kumar S, "Review on Prevention of Data Leakage in Cloud Server by Utilizing Watermarking and Double Encryption Techniques," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1619-1625, doi: 10.1109/ICACCS57279.2023.10112767.

[3] Devi, B. Padmini, and S. Kannadhasan. "Preventing Data Leakage in Cloud Servers through Watermarking and Encryption Techniques." (2023). DOI: https://doi.org/10.21203/rs.3.rs-3036586/v1

[4] Karthik, B., K. Sai Kumar, and M. Rajashekar. "Data Leakage Discovery in Cloud Using Watermark Fashion.", ISSN: 2321-9653, Volume 11 Issue II, Feb 2023.

[5] Alshutayri, Areej. "Fraud Prediction in Movie Theater Credit Card Transactions using Machine Learning." Engineering, Technology & Applied Science Research 13, no. 3 (2023): 10941-10945.

[6] Kunduru, Arjun Reddy. "THE PERILS AND DEFENSES OF ENTERPRISE CLOUD COMPUTING: A COMPREHENSIVE REVIEW." Central Asian Journal of Mathematical Theory and Computer Sciences 4, no. 9 (2023): 29-41.

[7] Alemami, Yahia, Ali M. Al-Ghonmein, Khaldun G. Al-Moghrabi, and Mohamad Afendee Mohamed. "Cloud data security and various cryptographic algorithms." International Journal of Electrical and Computer Engineering 13, no. 2 (2023): 1867.

[8] Kumar, A. Vijaya, Koppu Monica, and Krishnaveni Mandadi. "Data Privacy Over Cloud Computing using Multi Party Computation." In 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), pp. 262-267. IEEE, 2023.

[9] Tian, Yun, and Andres F. Romero Nogales. "A Survey on Data Integrity Attacks and DDoS Attacks in Cloud Computing." In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0788-0794. IEEE, 2023.

[10] Vlodymyrovych, Marchuk Artem, Larabi Fouad, and Yakduva Usman Hassan. "DATA PROTECTION IN THE PUBLIC CLOUD WITH ENCRYPTION AND A THIRD-PARTY AUDITOR." In The VI International Scientific and Practical Conference «Modern ways of solving the problems of science in the world», February 13–15, Warsaw, Poland. 445 p., p. 379.

[11] Abdullayeva, Fargana. "Cyber resilience and cyber security issues of intelligent cloud computing systems." Results in Control and Optimization 12 (2023): 100268.

[12] Guo, Jian, and Hua Guo. "Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing." Symmetry 15, no. 5 (2023): 988.

[13] Kusunose, Mayumi, and Kaori Muto. "Public attitudes toward cloud computing and willingness to share personal health records (PHRs) and genome data for health care research in Japan." Human Genome Variation 10, no. 1 (2023).

[14] Rana, Muhammad Ehsan, Tzung Maw Yik, and Vazeerudeen Abdul Hameed. "Cloud Computing Adoption in the Banking Sector: A Comparative Analysis of Three Major CSPs." In 2023 IEEE 6th International Conference on Big Data and Artificial Intelligence (BDAI), pp. 244-250. IEEE, 2023.

[15] Logeswaran, K., and M. Gunasekar. "Enhancing the Credit Card Fraud Detection Using Decision Tree and Adaptive Boosting Techniques." In Intelligent Systems Design and Applications: 22nd International Conference on Intelligent Systems Design and Applications (ISDA 2022) Held December 12-14, 2022-Volume 3, vol. 716, p. 358. Springer Nature, 2023.

[16] ALQAHTANI, KHOLOD SAEED, AZZAM MASHHEN ALBALAWI, and MOUNIR FRIKHA. "REVIEWING OF CYBERSECURITY THREATS, ATTACKS, AND MITIGATION TECHNIQUES IN CLOUD COMPUTING ENVIRONMENT." Journal of Theoretical and Applied Information Technology 101, no. 6 (2023).

[17] Ahmad, Hadeel, Bassam Kasasbeh, Balqees Aldabaybah, and Enas Rawashdeh. "Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS)." International Journal of Information Technology 15, no. 1 (2023): 325-333.

[18] Nguyen, Lam D., James Hoang, Qin Wang, Qinghua Lu, Sherry Xu, and Shiping Chen. "Bdsp: A fair blockchain-enabled framework for privacy-enhanced enterprise data sharing." In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-9. IEEE, 2023.

[19] TOUMI, HICHAM, FATIMA ZAHRA FAGROUD, KHADIJA ACHTAICH, FATIMA LAKRAMI, and MOHAMED TALEA. "COOPERATIVE TRUST FRAMEWORK BASED ON HY-IDS, FIREWALLS, AND MOBILE AGENTS TO ENHANCE SECURITY IN A CLOUD ENVIRONMENT." Journal of Theoretical and Applied Information Technology 101, no. 10 (2023).

[20] Sai, Kotireddy Yazna, Repalle Venkata Bhavana, and Natarajan Sudha. "Detection of Fraudulent Credit Card Transactions Using Deep Neural Network Check for updates." Soft Computing: Theories and Applications: Proceedings of SoCTA 2022 627 (2023): 185.

[21] Attivilli, Ravali, and Angel Arul Jothi. "Serverless Stream-Based Processing for Real Time Credit Card Fraud Detection Using Machine Learning." In 2023 IEEE World AI IoT Congress (AIIoT), pp. 0434-0439. IEEE, 2023.

[22] Yazna Sai, Kotireddy, Repalle Venkata Bhavana, and Natarajan Sudha. "Detection of Fraudulent Credit Card Transactions Using Deep Neural Network." In Soft Computing: Theories and Applications: Proceedings of SoCTA 2022, pp. 185-195. Singapore: Springer Nature Singapore, 2023.

[23] Mirhashemi, Qazaleh Sadat, Negar Nasiri, and Mohammad Reza Keyvanpour. "Evaluation of Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison." In 2023 9th International Conference on Web Research (ICWR), pp. 247-252. IEEE, 2023.

[24] Jain, Anjali, Srishty Mittal, Apoorva Bhagat, and Deepak Kumar Sharma. "Big Data Analytics and Security Over the Cloud: Characteristics, Analytics, Integration and Security." In Security and Risk Analysis for Intelligent Edge Computing, pp. 35-66. Cham: Springer International Publishing, 2023.

[25] Talaat, Fatma M., Abdussalam Aljadani, Bshair Alharthi, Mohammed A. Farsi, Mahmoud Badawy, and Mostafa Elhosseini. "A Mathematical Model for Customer Segmentation Leveraging Deep Learning, Explainable AI, and RFM Analysis in Targeted Marketing." Mathematics 11, no. 18 (2023): 3930.