International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

Secure Digital Information Forward Using Highly Developed AES Techniques in Cloud Computing

A. N. Arularasan[1], E. Aarthi[2], S.V. Hemanth[3], N. Rajkumar[4], T. Kalaichelvi[5]

[1]Department of Artificial Intelligence and Data Science, Panimalar Engineering College,Chennai - 600 123,Tamil Nadu,India. Email:arularasan@live.com (Corresponding Author)

[2]Assistant professor, Department of Computer Science,SRM Institute of Science and Technology,Kattankulathur, Chennai,India, Email: aarthi.devpal@gmail.com

[3]Associate Professor,Department of Computer Science and Engineering,Hyderabad Institute of Technology and Management,Medchal-Malkajgiri, Telangana 501401,India. Email: hemanth.sandapaga@gmail.com

[4]Department of Computer Applications , PSNA College of Engineering and Technology,Dindigul.Tamilnadu-624622, India. Email: nrajkumar@psnacet.edu.in

[5]Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai- 600123, India , Email: Kalaichelvi2012@gmail.com

Abstract— Nowadays, in communications, the main criteria are ensuring the digital information and communication in the network. The normal two users' communication exchanges confidential data and files via the web. Secure data communication is the most crucial problem for message transmission networks. To resolve this problem, cryptography uses mathematical encryption and decryption data on adaptation by converting data from a key into an unreadable format. Cryptography provides a method for performing the transmission of confidential or secure communication. The proposed AES (Advanced Encryption Standard)-based Padding Key Encryption (PKE) algorithm encrypts the Data; it generates the secret key in an unreadable format. The receiver decrypts the data using the private key in a readable format. In the proposed PKE algorithm, the sender sends data into plain Text to cypher-text using a secret key to the authorized person; the unauthorized person cannot access the data through the Internet; only an authorized person can view the data through the private key. A method for identifying user groups was developed. Support vector machines (SVM) were used in user behaviour analysis to estimate probability densities so that each user could be predicted to launch applications and sessions independently. The results of the proposed simulation offer a high level of security for transmitting sensitive data or files to recipients compared to other previous methods and user behaviour analysis.

Keywords : Support Vector Machine (SVM), AES-based Padding Key Encryption (PKE) algorithm, Denial of service (DOS), Inverse (Inv) - Mix-columns, Redact able Signature-Based Public Auditing Scheme (RSPAS).

I. INTRODUCTION

Cloud computing is a fad that allows users to use cloud services at any time, from any location, and on demand. Cloud computing offers services like virtualized network capacity, storage, development environments, and resource allocation and reallocation. Cloud services can be bought or free from companies like Amazon. The use of cloud services has significantly increased. With cloud computing, large amounts of stored data must be transferred quickly and securely. In other words, if the Data is accessed frequently, the address sequence or access pattern is hidden [1]. As a result, it cannot be easy to devise a plan to effectively conceal data access patterns or ensure that shared stored data cannot be discovered. To allow multiple cloud computing users to share data, a privacy-preserving and untraceable strategy are proposed that uses sloppy random access memory and a proxy encryption algorithm. In recent years, providing security for user data has become increasingly challenging due to the increased use of cloud services. There is a high probability of data loss or external intrusion, which makes the Data even more vulnerable.

Providing security during data transmission and storage is part of providing users with secure data. Data storage is the subject of existing methods for providing data security.

Discusses the cloud infrastructure and system based on N-tier architecture. The N-tier lead the multi-client and multi-server technology, which has been entirely distributed server applications. Here user-1, user-2, and user-3 are the number of clients or users of cloud networks. The third-party auditor should analyze the behaviour of clients or users. Routers have been used for interfaces between users and servers.

Novelty of the paper:

- This is the improves the cloud user security and expands the security.
- AES-based encryption to support to improve the security next level of the cloud networks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

- The SVM is a data mining algorithm for user behaviors and behaviour analysis based on low-level and high-level trust users.

II. RELATED WORKS

The objective is to stop third parties from accessing the cloud server data. The data storage server can be used for authentication and verification that the owner's data are accurately stored using the proposed system's Remote Data Integrity (RDIC) feature [2].

We present an Effective Audit Technique (EA) for user revocation and security auditing in the private cloud. Collaboration tolerance. Our system is risk-free and provides quick user shutdown and public verification options. [3].

Dual servers ensure that no server can independently access all data by employing secure two-way computing. Under the proposed plan, the data cannot be recovered if lost during transmission to the user. The data owner adds a random number during uploading to verify identity and prevent malicious deletion. [4].

Described how the robustness of CORBA to a discrete logarithmic approximation was diminished and gave a comprehensive analysis of its security. However, his original conservation reduction in this article—for discrete logs—is incorrect. Corba noise cannot be calculated using the discrete logarithmic approximation. [5].

Use a selection of Space's storage services to manage large files effectively. In addition, developed a Byzantine script data centre lease protocol. We evaluate bioinformatics' most effective Big Data workflows using simulated micro and application-based benchmarks. The findings demonstrate that our original design is practical and performs 2.5 times more effectively than other cloud-based solutions [6].

The Industrial Internet's data transfer and privacy protection are proposed in this document securely and effectively. A cloud computing layer is added between the Internet's industrial cloud and

Detection layer. It deals with data processing and integration, new encryptions and decryptions, mutual authentication, and device trust [7].

. The protocol developed in this article can satisfy the security requirements of ORAM and proxy rewriting, as demonstrated by the security analysis. Theoretical and experimental testing has shown that the proposed method for group data transfer in cloud computing is safe and effective. [8].

Users can save the settings for particular sub-policies for the first encryption and use them again for subsequent data encryptions, significantly lowering the amount of computational work required. This is because the built-in access policies also cover the child policy. [9].

For developing network-based data transmission systems, here we develop an effective identity-based transmission encryption scheme that simultaneously achieves data confidentiality and identity privacy. Authorized data recipients in the proposed data transfer system are known only to the data owner. [10].

However, because standard anonymization strategies may not consider various usage scenarios, these data erasure tools introduce new security risks. As a result, propose a brand-new method with signatures that can be written. Cloud project servers do not need to exchange signatures directly, sharing sensitive data. [11].

This study looks at two distinct categories of data users and the various roles and actions that can be performed with outsourced data. Finally, the validity, control, and accuracy of the externalized data are all guaranteed by this work. The test results demonstrate our solution's scalability and performance. [12].

Utilizing blockchain, this paper proposes an effective method for protecting access records. The results demonstrated that our model could effectively increase the source data's level of security when applied to a broad framework that was designed, tested, and evaluated. [13]

To address these issues, propose a model system for securely sharing data from digital twins. The block chain is used to verify the data, and cloud computing transfers Data effectively in the proposed system model. Formal and informal approaches, like BAN logic and the AVISPA simulation tool, are utilized in our investigation of the proposed protocol's security.. [14].

To address critical leakage issues, our project ensures a novel concept of data privacy for IoT data at the item level. We accomplish these objectives by employing various coding and optimization techniques. Our main tests combine system implementation with full-scale emulation to check our design's security and performance. [15].

The structural characteristics of social networks, users' social behaviour, and relationships with other users are just a few of the many topics studied in social network research. This work focuses on social networks because mobile communication networks are closely associated with everyday life. [16].

Security, on the other hand, is a significant roadblock to cloud computing's expansion. This investigation focuses on developing a joint learning-based collaborative intrusion detection system (IDS). It identifies various cloud system attacks using inactive cloud resources and weak classifiers. [17].

The use of IT infrastructure for business purposes has grown in recent years thanks to the digital age. By moving on-premises workloads to data centres that can be accessed from

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

anywhere over the Internet and reducing complexity, cloud infrastructure plays a significant role. [18].

III. PROPOSED METHODOLOGY

The security of user-supplied data sent to cloud servers is the primary focus of the proposed system for cloud server security. Data will be encrypted using AES encryption as it is sent to cloud servers for storage. The external auditor is responsible for user authentication verification and selects the server to store user data. After the user has been verified and the available servers have been listed, the external auditor role is ended in a specific transaction. The external auditor needs to learn the system's encryption and decryption procedures. Figure 2 illustrates the proposed cloud security model.

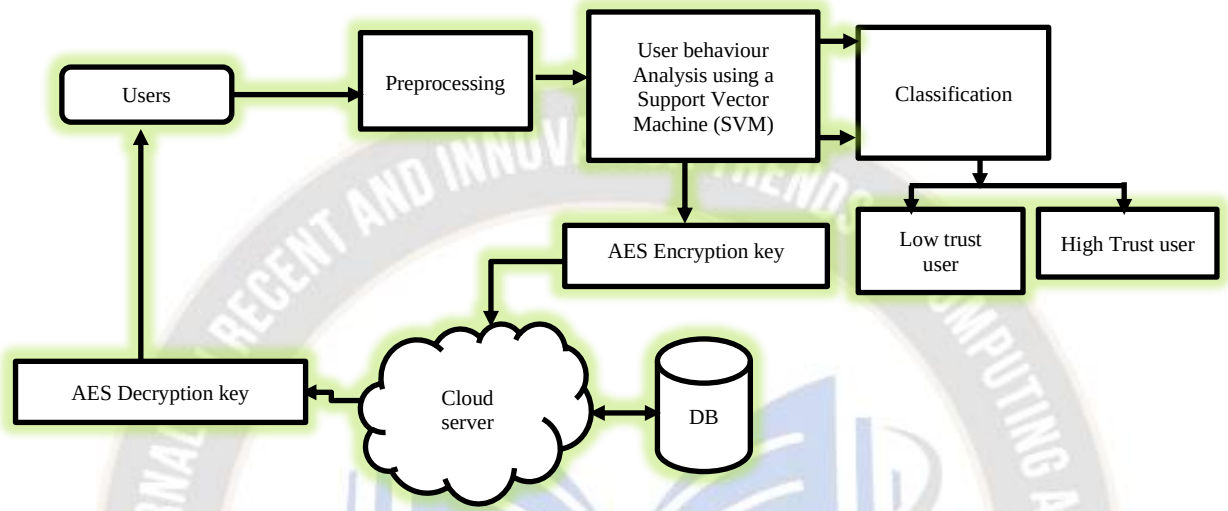

Fig.1. Proposed system Architecture

Figure.1 defines the Cloud User management used to initialize how much using the cloud server. The users get the inputs request to the cloud server, create the users, and the user responses of the cloud network and the general user's cloud processing are managed here

The following processes of preprocessing, and the User behaviour Analysis using a Support Vector Machine (SVM), AES-based Padding Key Encryption (PKE) algorithm is using encryption of the data and text, Cloud Server analysis and the AES-based Padding Key Decryption (PKD) algorithm is using decryption of the data and text.

A. *User behaviour Analysis using Support Vector Machine (SVM)*

The support vector machine algorithm preprocesses data collection, data or content checking and evaluates the input data. Whether the contents are supported or not, check the preprocessing. This algorithm has verified all types of data and classification support. Collect the user input data, review them, and send them to the server.

Input for the outcome of the data P^*, $P^*$is the outcome of binary data.

Machine learning enables computers to carry out tasks independently and effectively without explicit instructions. The input data are essential for machine learning.

It infers the result and learns patterns from the provided input data. It is a natural process to learn from previous experiences, from previous information, and to learn in stages or phases. Machine learning algorithms mimic this learning strategy.

Sample data are used as input by algorithms for SVM (Support vector Machine). This Data Model is referred to as dataset. These training data are used to build a mathematical model. A machine learning model learns to recognize patterns, relationships, and correlations from this training data in records. Using this test data, the accuracy of the machine learning model can be evaluated. The accuracy of a model is a measure of its degree of training. As the accuracy increases, model performance rises. Another factor that affects model performance is model data.

The SVM algorithm has been classifying the cloud user behaviour analysis; the analysis based on Normal users and malicious users is counted, and then after the algorithm has classified the user behaviours. The following algorithm steps are:

Support Vector Machine (SVM) Classification
Step1 Dataset P* is the out-of-the-user behaviours
Step2
Train the SVM model
$P \leftarrow P^*$
Step3: While $P^* \geq 2$ do
$SVM_P \leftarrow SVM$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

With the optimized tuning parameter for the P variable and observation of the Data.

$w_p \leftarrow$ calculate the vector of the SVM$(w_{p1}, w_{p2} \ldots w_{pp})$

User Rank. criteria $\leftarrow (w_{p1}^2 \ldots . . w_{pp}^2)$

min. user. rank. criteria $\leftarrow$ lowest user. rank. criteria vectors;

Remove, min. user. rank. criteria;

user. $\text{rank}_p \leftarrow$ min. user. rank. criteria;

$P \leftarrow P - 1$;

End

Step4:

user. rank_p $\leftarrow$ variable in the data $\nexists$(user. rank_2, … user. rank_{p*})

Step5:

return (user. rank_p …. user. rank_{p*})

Step6:

End

Herein, this algorithm is a linear kernel in a model for binary classification; p* is the user behaviour data set, get the input to train the classification$\leftarrow P - 1$, then while loop is used checked the condition p. Then after turning the parameter P into looping, w_p is the vector collection of SVM. The variable is assigned to the user parameter

user. $\text{rank}_p \leftarrow$ variable in the data $\nexists$(user. rank_2, … user. rank_{p*}) - (1)

Then return the (user. rank_p). This algorithm classifies rank-based or high-trust users; low-trust users are identified.

As seen in the illustration that came before it, there are two input data sets. Operations data and login data make up the first and second, respectively. They are both system logs from when a user logs in until they log out. From the input data, significant features are extracted through the feature extraction process. After many elements are removed, the two data sets are combined. The model is trained and tested with the combined data set through machine learning. Rules derived from SVM are used to classify users. Confidence ratings were given to rated users.

There are a total of six characteristics in the login and operations data. Twelve features are present in total after feature extraction. Four machine learning algorithms are trained and tested with this feature data. The algorithm's prediction accuracy is determined for each machine. The data are tested with the best precision and the appropriate model. This model's accuracy is taken into consideration for further classification. We have developed rules to divide users into six categories, drawing on the SVM rules. The model's output consists of these six categories. They are,

a) Very High Trust
b) High Trust
c) High Medium Trust
d) Medium Trust
e) Low Trust
f) Very Low Trust

With the usage, users' trust value is either increased or decreased. Trust value goes higher when the users do not exhibit any anomalies.

TABLE I. CLASSIFICATION OF USER BEHAVIOR TRUST CATEGORIES

values	Trust level
0.9-1.0	Very High Trust
0.75-0.9	High Trust
0.5-0.75	High Medium Trust
0.25-0.5	Low Medium Trust
0.1-0.25	Low Trust
0.0-0.1	Very Low Trust

Machine learning algorithms have been applied to our models, with the highest accuracy chosen. Now, look at the number of users who are logged in in Table 1. Six users' behavioural analyses are discussed in this section. The confidence level is defined as very high confidence, high confidence, medium-high confidence, medium-low confidence, low confidence, and shallow confidence. The value is a range of confidence values.

When providing services to users, user and resource security should also be a top priority. Assurance can be enhanced by incorporating user behaviour into existing security technology. The primary objective of the design and construction of this model was to assess service customers' trustworthiness. Active attacks can be stopped immediately if user behaviour is discovered early. The model produces the six distinct user confidence classes as its final output. The people who use the input data are in these six categories.

B. AES-based Padding Key Encryption (PKE) algorithm

User identifications, such as entering a secret key or secret answer to verify an individual's identity, have been the subject of extensive research. This security measure still has a flaw because identities can be stolen. For user identification, a random key based on AES is an option. A practical method for determining the user is this one. However, this feature must be present on all systems where the user conducts activity.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

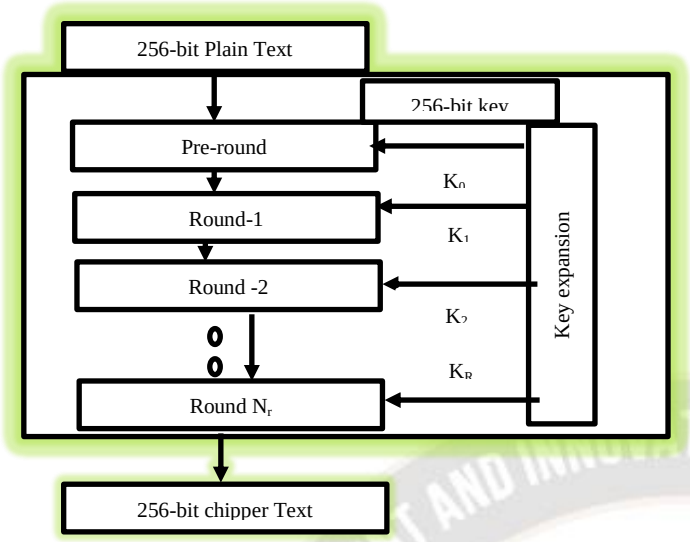

Fig.2. Key routing steps

However, security has been a problem caused by the expansion of mobile networks. Denial of service (DoS), Identity theft, and network spoofing are all examples of security damage. Figure 2 shows that AES-253 encrypts and decrypts blocks of messages with a 256-bit key, whereas AES-256 encrypts and decrypts messages with a 256-bit key. A legend with 256 bits key.

10 cycles, 12 cycles, and 14 cycles, respectively. In many processing steps, a round includes replacing, transposing, and scrambling the input plaintext into the final cipher text output. Robust encryption algorithms support these virtual machines' trust and security features.

AES 256bit Encryption Algorithm

Step1:

Plain text P* -> P

Step2:

Plaint text P+= round key

Step3:

If $i=N_r$ then // condition is true //

Sub bytes P // text convert to bytes //

Shift rows += Round key (N_r)

Shift rows += Round key (N_r)

Step4:

Cipher Text -> P // convert file stored in p

Step5:

Else // condition false //

Mix-columns += Round key (i)

Step6:

Server <= Mix-columns+p // send data to server //

Step7:

End

In these Algorithm define the AES 256-bit key encryption system, discuss the encryption process, the input data, user behaviour data or dataset P*. The N_r is no of round key process. P* is taken from the plain Text, and then the method of secret critical updates for plain Text. The keys and plain Text have been converted into encrypted byte values. The following process of checking condition "if (i=Nr)", the situation is true means round key steps start. After that, randomly select the round key from the mix column, and plain Text is encrypted. The encrypted chipper text p* is sent to the cloud server.

C. AES-based Padding Key Decryption (PKD) algorithm

The Figure.4 defines the AES 256-bit key decryption system and discusses the decryption process and the input data of chipper text; the keys and encrypted chipper text have been converted into plain Text. Before checking the following method of checking condition "if (i=Nr-1)", the condition is valid means round key steps start.

Inverse (Inv) -Mix-columns values on the table. After that, randomly check the round key from the Inv-Mix columns. The key matched means chipper text is decrypted. The encrypted chipper text p* is sent to the user from the cloud server.

The cloud network's security performance is the subject of this chapter. The performance is based on the analysis and calculation of the cloud networks using a variety of approaches. The outcome looked at the various versions of Cloud User Security Analysis and Cloud Security Analysis. A Privacy-Preserving and Untraceable Group Data Sharing Scheme (PPUG), EA (Evolutionary Algorithm (EA), Redact able Signature-Based Public Auditing Scheme (RSPAS), and Advanced Encryption Standard (AES) must be compared to the following algorithms. The user's Behaviour analysis using the following algorithms are compared Logistic Regression, Decision Tree, Random Forest, support vector machine(SVM)

IV. RESULT AND DISCUSSION

The cloud network's security performance is the subject of this chapter. The performance is based on the analysis and calculation of the cloud networks using a variety of approaches. The outcome looked at the various versions of Cloud User Security Analysis and Cloud Security Analysis. A Privacy-Preserving and Untraceable Group Data Sharing Scheme (PPUG), EA (Evolutionary Algorithm (EA), Redact able Signature-Based Public Auditing Scheme (RSPAS), and Advanced Encryption Standard (AES) must be compared to the following algorithms. The user's Behaviour analysis using the following algorithms are compared Logistic Regression, Decision Tree, Random Forest, support vector machine(SVM).

Table.II. Simulation Parameters of The Proposed Method

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4s
DOI: https://doi.org/10.17762/ijritcc.v11i4s.6315
***Article Received**: 28 December 2022 **Revised**: 30 January 2023 **Accepted**: 10 February 2023*

B. *Cloud Security Analysis*

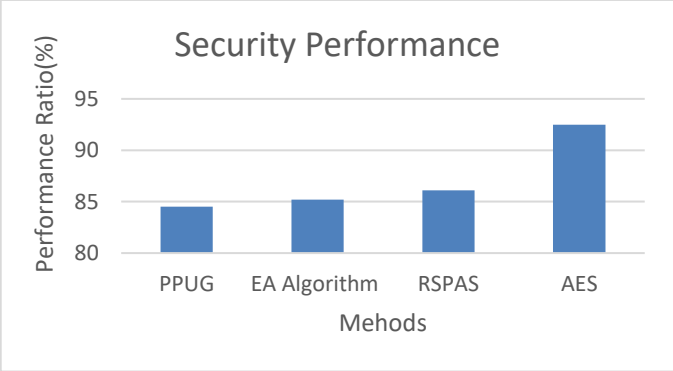

Fig.4. User security performance

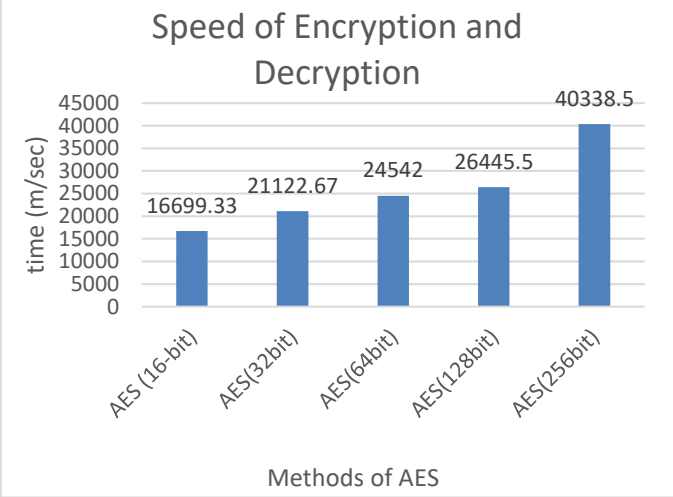

Fig.5. Time and speed of Encryption and Decryption

The Equation (3) calculate the total throughput. Figure.5 discuss the performance of Encryption and Decryption time speeds. AES-16bit encryption and decryption time method is 16699.33 m/sec taken, and AES-32bit encryption and decryption time is 21122.67. m/sec taken, AES-64bit encryption and decryption time is 24542 m/sec taken, AES-128bit encryption and decryption time is 26445.5 m/sec taken, AES-256bit encryption and decryption time is 40338.5 m/sec taken.

V. CONCLUSION

Digital Data transmission and storage are made more secure by the AES-based secure model proposed for cloud data security. During the bulk data flow, the system is unavailable due to the use of AES encryption for data transfer. You prevent intruders from entering your network by acting as a third party by denying access to third parties. The proposed changes to the encryption implementation and critical expansion encrypt data with solid diffusion and scattering properties, even though the original AES algorithm is extremely secure. The AES algorithm's security is enhanced by bolstering the cryptographic system's resistance to attacks through slight modifications. As a result, the proposed strategy provides cloud-based user data with effective AES-based encryption methods performance is 92.5%. Then user behaviour and the SVM best performance of average is 98.12981%.

REFERENCE

[1]. J. Shen, H. Yang, P. Vijayakumar and N. Kumar, "A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2198-2210, 1 July-Aug. 2022, DOI: 10.1109/TDSC.2021.3050517.

[2]. S. Sushma, P. Srilatha and G. Srinivas, "Efficient Integrity Checking and Secured Data Sharing in Cloud," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2022, pp. 1-4, DOI: 10.1109/ICSES55317.2022.9914256.

[3]. V. K. Singh, N. Bharathiraja, S. Arun, D. B. David, R. Krishnamoorthy and R. Thiagarajan, "Secure Shared Data in the Private Cloud With an EA Algorithm," 2022 8th International Conference on Smart Structures and Systems (ICSSS), 2022, pp. 1-6, DOI: 10.1109/ICSSS54381.2022.9782299.

[4]. X. Luo, H. Wang, J. Dong, C. Zhang and T. Wu, "Achieving Privacy-preserving Data Sharing for Dual Clouds," 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybernetics (Cybernetics), 2022, pp. 139-146, DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00059.

[5]. J. Chang, B. Shao, Y. Ji and G. Bian, "Comment on “A Lightweight Auditing Service for Shared Data With Secure User Revocation in Cloud Storage”," in IEEE Transactions on Services Computing, vol. 15, no. 5, pp. 2633-2634, 1 Sept.-Oct. 2022, DOI: 10.1109/TSC.2021.3056660.

[6]. R. Mendes, T. Oliveira, V. Cogo, N. Neves and A. Bassani, "Charon: A Secure Cloud-of-Clouds System for Storing and Sharing Big Data," in IEEE Transactions on Cloud Computing, vol. 9, no. 4, pp. 1349-1361, 1 Oct.-Dec. 2021, DOI: 10.1109/TCC.2019.2916856.

[7]. J. Li, D. Yang and K. Zhang, "Secure Data Sharing Algorithm for Privacy Protection of Industrial Internet," 2021 IEEE Conference on Telecommunications, Optics and Computer Science (TOCS), 2021, pp. 202-208, DOI: 10.1109/TOCS53301.2021.9688774.

[8]. J. Shen, H. Yang, P. Vijayakumar and N. Kumar, "A Privacy-Preserving and Untraceable Group Data Sharing Scheme in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 2198-

2210, 1 July-Aug. 2022, DOI: 10.1109/TDSC.2021.3050517.

[9]. k. Xue, N. Gai, J. Hong, D. S. L. Wei, P. Hong and N. Yu, "Efficient and Secure Attribute-Based Access Control With Identical Sub-Policies Frequently Used in Cloud Storage," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 635-646, 1 Jan.-Feb. 2022, DOI: 10.1109/TDSC.2020.2987903.

[10]. F. Wang, J. Wang and S. Shi, "Efficient Data Sharing With Privacy Preservation Over Lattices for Secure Cloud Storage," in IEEE Systems Journal, vol. 16, no. 2, pp. 2507-2517, June 2022, DOI: 10.1109/JSYST.2021.3077236.

[11]. S. Li, J. Han, D. Tong and J. Cui, "Redactable Signature-Based Public Auditing Scheme With Sensitive Data Sharing for Cloud Storage," in IEEE Systems Journal, vol. 16, no. 3, pp. 3613-3624, Sept. 2022, DOI: 10.1109/JSYST.2022.3159832

[12]. C. Hahn, J. Kim, H. Kwon and J. Hur, "Efficient IoT Management With Resilience to Unauthorized Access to Cloud Storage," in IEEE Transactions on Cloud Computing, vol. 10, no. 2, pp. 1008-1020, 1 April-June 2022, DOI: 10.1109/TCC.2020.2985046.

[13]. E. B. Sifah, Q. Xia, K. O. -B. O. Agyekum, H. Xia, A. Smahi and J. Gao, "A Blockchain Approach to Ensuring Provenance to Outsourced Cloud Data in a Sharing Ecosystem," in IEEE Systems Journal, vol. 16, no. 1, pp. 1673-1684, March 2022, DOI: 10.1109/JSYST.2021.3068224.

[14]. S. Son, D. Kwon, J. Lee, S. Yu, N. -S. Jho and Y. Park, "On the Design of a Privacy-Preserving Communication Scheme for Cloud-Based Digital Twin Environments Using Blockchain," in IEEE Access, vol. 10, pp. 75365-75375, 2022, DOI: 10.1109/ACCESS.2022.3191414.

[15]. S. Qi, Y. Lu, W. Wei and X. Chen, "Efficient Data Access Control With Fine-Grained Data Protection in Cloud-Assisted IIoT," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2886-2899, 15 Feb.15, 2021, DOI: 10.1109/JIOT.2020.3020979.

[16]. S. -S. Zhang, X. Liang, Y. -D. Wei and X. Zhang, "On Structural Features, User Social Behavior, and Kinship Discrimination in Communication Social Networks," in IEEE Transactions on Computational Social Systems, vol. 7, no. 2, pp. 425-436, April 2020, DOI: 10.1109/TCSS.2019.2962231.

[17]. P. Mehetrey, B. Shahriari and M. Moh, "Collaborative Ensemble-Learning Based Intrusion Detection Systems for Clouds," 2016 International Conference on Collaboration Technologies and Systems (CTS), 2016, pp. 404-411, DOI: 10.1109/CTS.2016.0078.

[18] P. Jha and A. Sharma, "Framework to Analyze Malicious Behaviour in Cloud Environment using Machine Learning Techniques," 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-12, DOI: 10.1109/ICCCI50826.2021.9402671.