International Journal of Computer and Engineering Optimization (IJCEO)
Volume 1, Issue 1, September – October (2023)

RESEARCH ARTICLE

DEEP LEARNING BASED AUTHENTICATION SECURE DATA STORING IN CLOUD COMPUTING

M. Prabhu[1, *], G. Revathy[2] and R. Raja Kumar[3]

[1]Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai India.
[2]Department of Electronics and Instrumentation Engineering, Sengunthar Engineering College, Erode, Tamil Nadu 638057, India
[3]Department of Mathematics, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu 600119 India.

[*]*Corresponding e-mail: prabhu.ece05@gmail.com*

Abstract – To communicate organizationally important data among working units in a federated cloud environment, secure mutual authentication is a crucial necessity. The administration of data while preserving its usefulness and security system is a worry for the cloud owner. Cloud data sharing is becoming more and more popular as a viable way to give people simple access to data. supported by positive advances in cloud technology. Yet, as more businesses and customers store their data on cloud servers, it poses a growing threat to user privacy and data security. People are inclined to encrypt information before sending it to the cloud in order to ensure its confidentiality. Yet the data processing has gotten challenging due to broad encryption methods. In order This paper provides a novel mutual authentication mechanism that combines deep learning-based recognition and control of security breaches to enable secure communication between participating entities. Convolutional Neural Networks (CNN) for online threat detection with RSA Cryptography and Schnarr's signature scheme-based public-key encryption technologies. A network intrusion dataset from the Canadian Institute for UNSW-NB15 is used to measure performance, and the AVISPA security analysis tool confirms its effectiveness in comparison to other methods in terms of security features and communication costs.

Keywords *– RSA cryptography; mutual authentication; AVISPA security analysis, Schnorr signature; Convolutional neural networks (CNN), threat, encrypted data*

1. INTRODUCTION

Securing every online communication between sending and receiving entities has become a requirement in order to guarantee secure and efficient online commerce or data collaboration. As a result, to enable secure key exchange and the development of secure sessions during data sharing, a reliable mutual authentication system is required. In the previous year, 47% of firms suffered security attacks or failed compliance audits, according to Thales Report 2020. In addition, a multi-server environment has added new difficulties and sparked security flaws. Numerous researchers have put forth a variety of security solutions in response to online data exchange security flaws, these include mutually authenticated safe secret key exchange, secure data storage and sharing, safeguarded credential storage, techniques for granting access to data, and safe authentication protocols.

Clients that save their data on the cloud may easily and rapidly retrieve it without needing to be specialists in the setup and upkeep of the equipment or architecture. In comparison with desktop computer, cloud computing offers significantly greater power. But it also introduces additional privacy and security problems because users lose control over their data when it is outsourced and they no longer have physical access to it. Full access to cloud services exposes customers' data to several dangers and hostile attacks, and security breaches are common as a result.

Despite these benefits, keeping personally identifiable information in a cloud environment greatly increases the need for security. As sensitive data is transferred from the federated domain to the distribution domain, this raises questions about regulatory compliance. Big data technologies can be used to their full potential, however, issues with privacy and security must be addressed first. Also, as the cloud is based on the pillars of two fundamental foundations, such as cloud computing and networking, Internet connectivity and infrastructure are crucial. The network can be utilized for cloud computing and other applications for numerous cloud applications.

Digital data is now protected by encryption. The goal of this area of computer science is to transform data into understandable representations for only authorized users. Basic cryptography is demonstrated with an encrypted message where the letters have been replaced with other characters. In the presence of adversaries, or malicious outsiders, cryptography enables a secure route of communication. A key (also referred to as cipher text) and an algorithm are used in encryption to convert a plaintext

input into an encrypted output. The three primary objectives of cryptography are data privacy, data authenticity, and data integrity.

In order to overcome the issues with online data sharing, a mechanism for improved mutual authentication is created in this study. It is based on the trusted cloud server's integration of RSA cryptography and deep learning techniques. It is advised to follow the correct registration procedure, engage in deep learning, and use key agreement and RSA cryptography for threat detection during the session setup and password change stages, respectively. For secure online data sharing. The principal contributions of the planned work are summarized as follows:

- An RSA Cryptography and deep learning-based Authentication Protocol is proposed to facilitate data exchange among users on federated cloud servers.
- At a trusted cloud server, CNN is used to develop an online threat detection system to mitigate denial of service attacks.
- Verification using AVISPA tool for security analysis and state-of-the-art protocol comparison with the suggested protocol.

The remaining portions of this work are arranged as follows: Section 2 reviews the literature on earlier studies; Section 3 provides a detailed analysis of the suggested work; Section 4 offers the findings; and Section 5 concludes.

2. LITERATURE SURVEY

In 2018 Olufemi Olakanmi, O. and Oke, S. [6] proposed a successful mutual authentication system for using diverse MCC services. With the proposed technique, cryptography operations can be integrated with voice signatures to create an effective mutual authentication scheme that eliminates key escrow issues while enabling authorized users to more affordably obtain varied MCC services. The assessments of security and performance indicate that our suggested system outperforms the two most recent state-of-the-art MCC service systems. We will use other penetration tests that are available in the future to investigate the scheme's security in more detail.

In 2019 Gupta, I., et. al.., [4] proposed a layered architecture based on sensitivity is effective for protecting data security and privacy in a cloud environment. Because of the multilayer security in the suggested design, cloud service providers experience less overhead overall. To evaluate the effectiveness of the layer-based strategy, experimental analysis is done. According to the experimental findings, processing 200 papers of 20 MB each took 437, 2239, 3142, and 3900 milliseconds for content that is successively public, private, and top-secret. The outcomes of the experiments demonstrate the accuracy, applicability, dependability, and effectiveness of the suggested strategy.

In 2019 Zhang, L.,[7] proposed a CP-ABE method with effective authority verification that protects privacy. Assuming the decisional linearity assumptions and the decisional BDHE issue, the suggested approach achieves selected security. a CP-ABE approach in the standard model that protects privacy. With constant-size private keys and brief cypher texts, the proposed approach has numerous advantages over the existing ones. Moreover, just four pairing computations are required for decryption. The suggested approach also allows for authority verification without any privacy leakage.

In 2019 Han, S.,[5] proposed to a group exchanging secret key prevents unauthorized access to shared data and the communication process. management protocol (SSGK) is used. Data that is shared is encrypted using a group key in SSGK, and the group key is distributed secretly. According to in-depth security and performance assessments, Cloud storage reduces dangers to privacy and security and frees up around 12% of space.

In 2020 Butt, U.A., [2] proposed an analysis of machine learning (ML) techniques to address CC security risks, issues, and solutions; also, the usefulness of each method is evaluated based on its characteristics, advantages, and disadvantages. Algorithms for semi-supervised, supervised, unsupervised, and reinforcement learning are used to address cloud security issues. Security threats and attacks were examined as the most difficult problems in CC.

In 2021 Nassif, A.B. et al..,[1] proposed Security strategies and techniques for ML and the cloud. The three key research areas covered by the SLR's findings are I the different risks to cloud security, (ii) the ML methods used, and (iii) the performance outcomes. Furthermore, with a use rate of 16% and 14%, respectively, the two most common areas of cloud security are DDoS and data privacy.

In 2022 Reddy, S. et., al..,[3] suggested a state-of-the-art SaaS architecture that makes advantage of attack node mitigation. The Median Fitness-oriented Sea Lion Optimization algorithm (MFSLnO) is used to modify the weight and activation function during the Deep Belief Network (DBN) attack detection phase. The suggested method outperforms traditional approaches, achieving an 89% throughput and a 16% packet loss ratio.

3. PROPOSED METHODOLOGY

In this section a novel deep encrypt technique has been proposed to overcome the security while sharing data in cloud.The identification module and the encryption module are the two steps that make up the suggested technique. Whether it is an attack or not will be determined by the suggested strategy. The session will be stopped or cancelled if it is an attack.

3.1. Identification Module

There will be data theft during transmission when the data owner transmits information to the receiver initially. The historical data will be gathered in this module to discover the live data from the data owner, which will be provided for CNN classification.

3.1.1. CNN

The overall performance and complexity of a CNN structure may be influenced by a variety of hyper-

parameters, including the number and characteristics of hidden layers, pooling schemes, normalization plans, and cost functions. To train a CNN system for visualizing a landscape, additional reference annotations—also called labels or targets—and data from remote sensing were required. Convolution layers are more potent data structures that can be used with CNN-based training; however support vector networks and random forests are two examples of machine learning techniques that utilize relatively simple array-type data structures.

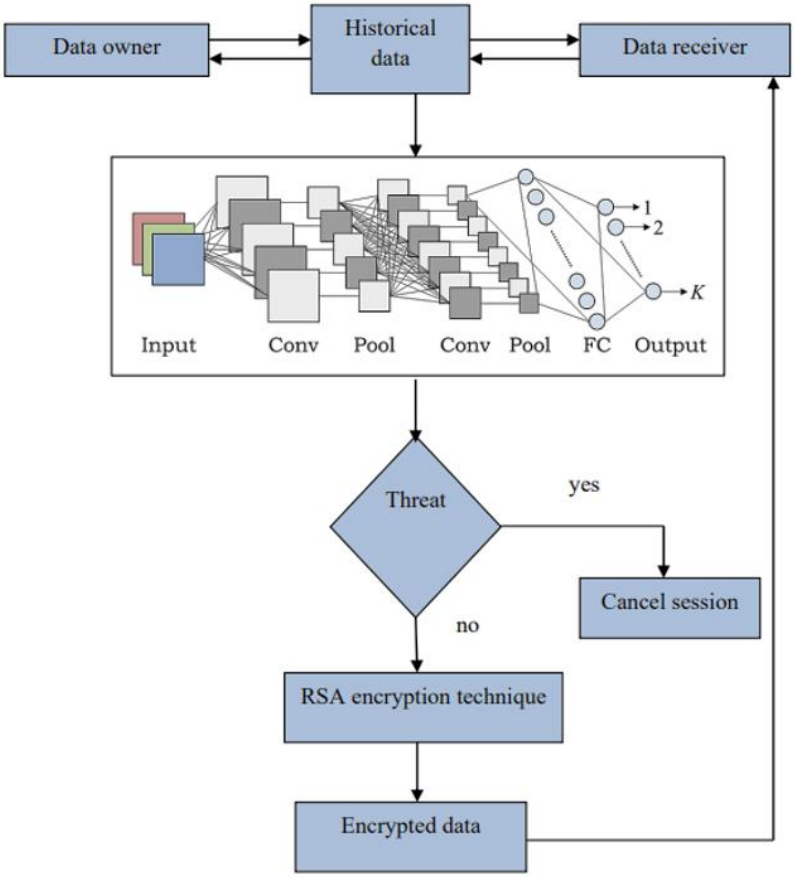

Figure 1. Block diagram of proposed methodology

In order to lower the number of pieces in that stimulus, the pooling method will fully reduce the insight along the spatial representation. The acquired features are typically dynamically down-sampled via additional-level methods within every multiple convolutional layer series. Max-pooling is the most common type of pooling procedure. Max-pooling aims for large activations rather than, say, average pooling. There are numerous distinct sorts of architectures that can be referred to by the term "CNN architecture," which outlines the potential connections between the neuronal or pooling layers of a CNN. As a result, CNNs are able to communicate a variety of opinions, many of which are influenced by their goals.

The convolutional layer will estimate as a scalar product the mass of the neurons whose output is related to certain input volume areas and the strength of the input volume-connected region. The corrected unit, also called ReLu, tries to stimulate the output from activating the previous layers by adding a "definite data" kernel operation (e.g., logarithmic kernel function). The fully connected layers are going to execute operations akin to those in traditional artificial neural networks (ANNs) with the goal of extracting output values of the kernel function which may be utilized for classification in the end. ReLu can also be used to enhance performance in between these layers.

3.2. Encryption Module

The RSA encryption method is used to encrypt the data. The difficulty of dissecting really large numbers determines how secure the RSA method is. The procedure using two enormously big prime numbers acts to create both the private key and the public key. According to estimates, it is just as difficult to decrypt Predicting the plaintext from the signal key and the cipher text is as difficult as calculating the product of two huge prime integers. The ISAKMP/Oakley design has considered using the RSA algorithm as a possible authentication technique. One essential element of the design is the Diffie-Hellman key exchange protocol.

To attain optimal effectiveness, the symmetric cryptographic algorithms and public key cryptography algorithms are always coupled. In other words, the DES key must be transmitted using an asymmetric key cryptosystem, such as RSA, and the confidential data must be supplied encrypted using a symmetric key cryptosystem. This uses two separate types of encryptions, high-speed DES and the practical and secure RSA key management scheme.

RSA is helpful for both authentication and encryption. The generated signature key for public key algorithms is only kept on the user's computer, which increases security compared to hash signatures. In order to provide localized components that are compatible with the end user's local OS, the RSA algorithm is implemented using C++.

Because there is currently no demonstration that breaking RSA would absolutely require factoring large numbers, it is not completely established in principle that RSA is equivalent to integer factorization. Instead, the security of RSA depends on how challenging integer factoring is. Several RSA variations are been shown to be interchangeable with integer factorization techniques. Hence, the data receiver will receive the encrypted data.

4. RESULT & DISCUSSION

The traditional numerical parameters given below have been used to evaluate the suggested model. Equations (1), (2), (3), and (4) were used to calculate accuracy, recall, specificity, and sensitivity, respectively. Equation (1) was used to calculate the accuracy.

4.1. Evaluation metrics

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Specificity = \frac{TN}{TN+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FP} \quad (3)$$

$$Percision = \frac{TP}{TP+FP} \quad (4)$$

For the provided data, there are four possible outcomes: true positive (TP), false positive (FP), false negative (FN), and true positive (TN). Positive labels are applied to false negative data, whereas positive labels are applied to actual positive data and classified accordingly. While TN data is labeled as negative and labeled as negative, false positive data is considered to be positive. The comparison graph is plotted below.,

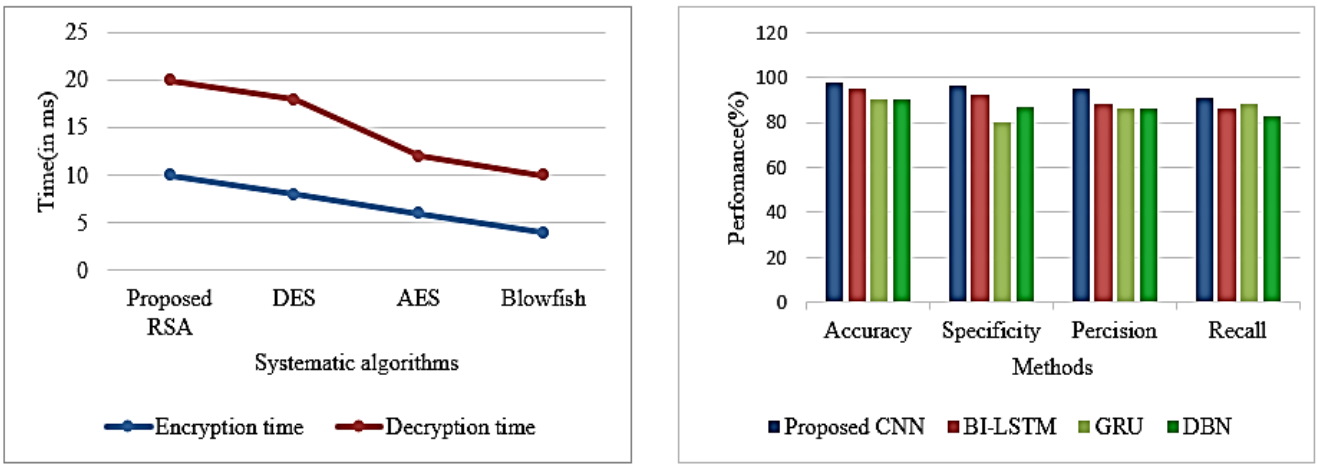

Figure 2. Comparative analysis of proposed methodology

In Figure 2, several metrics, such as recall, accuracy, specificity, and precision rate, are represented graphically as an overview of proposed and existing approaches. Viewing the graphs clearly shows that the proposed approach is appropriate for recognizing assaults and superior to all presently used methods. Sensitivity and specificity of the suggested approaches are 98.01% and 96.02%, respectively. The proposed framework outperformed the current BI-LSTM, GRU, and DBN in terms of sensitivity and specificity when compared to earlier models. A comparison graph for encryption and decryption time also analyzed.

5. CONCLUSION

Introducing a ground-breaking mutual authentication method for secure data transmission since the user's actual identification is frequently utilized session keys are never directly disclosed on the public network, it is founded on cryptography and deep learning. In this study, a unique mutual authentication technique is presented that combines RSA cryptography with deep learning-based convolutional neural networks (CNN) for online threat detection. Also, this mutual authentication system's security has been examined using the AVISPA security analysis tool. The findings show that the suggested protocol is inexpensive to compute with and secure from a wide range of security threats that could arise during online data sharing in a multi-cloud context.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

No funding was received to assist with the preparation of this manuscript.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for all of their careful, constructive and insightful comments in relation to this work.

REFERENCES

[1] A.B. Nassif, M.A. Talib, Q. Nasir, H. Albadani, and F.M. Dakalbab, "Machine learning for cloud security: a systematic review", *IEEE Access*, vol. 9, pp. 20717-20735, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] L. H. Merino, & M. Cukier, "An Approach for Preventing and Detecting Attacks in the Cloud", *In 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC)*, IEEE, pp. 165-175, 2020, December. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Reddy, and G.K. Shyam, "A machine learning based attack detection and mitigation using a secure SaaS framework", *Journal of King Saud University-Computer and Information Sciences*, vol.34, no.7, pp. 4047-4061, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] I. Gupta, N. Singh, and A.K. Singh. "Layer-based privacy and security architecture for cloud data sharing", *Journal of Communications Software and Systems*, vol.15, no.2, pp.173-185, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] S. Han, K. Han, and S. Zhang, "A data sharing protocol to minimize security and privacy risks of cloud storage in big data era", *IEEE Access*, vol.7, pp. 60290-60298, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] O. Olufemi Olakanmi, and S.O. Oke. "MASHED: Security and privacy-aware mutual authentication scheme for heterogeneous and distributed mobile cloud computing services", *Information Security Journal: A Global Perspective*, vol.27, no.5-6, pp.276-291, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] L. Zhang, Y. Cui, and Y. Mu. "Improving security and privacy attribute-based data sharing in cloud computing", *IEEE Systems Journal*, vol.14, no.1, pp.387-397, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] A.K. Singh, and D. Saxena. "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment", *Journal of Applied Security Research*, vol.17, no.3, pp.385-412, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. Karuppiah, A.K. Das, X. Li, S. Kumari, F. Wu, S.A. Chaudhry, and R. Niranchana. "Secure remote user mutual authentication scheme with key agreement for cloud environment", *Mobile Networks and Applications*, vol.24, pp.1046-1062, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] G. Wang, Q. Liu, and J. Wu. "Achieving fine-grained access control for secure data sharing on cloud servers", *Concurrency and Computation: Practice and Experience*, vol.23, no.12, pp.1443-1464, 2011. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

M. Prabhu, Associate Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, received his BE [ECE] degree from Anna University, Chennai in the year 2005, ME in communication systems from Anna University, Chennai in 2011 and Doctoral degree from Anna University, Chennai in the year 2023. He is having more than 18 years of experience in reputed engineering colleges. He has published 2 peer-reviewed International Journals, many papers at national and international conferences. Also, he has attended 50 FDPs, workshops, and seminars. His research interest lies in the field of wireless communications, Wireless sensor networks, Adhoc and sensor networks and 5G communications

G. Revathy received her M.E. degree from Kongu Engineering College, Anna University, India. She is now actively performing as an Assistant Professor in the Department of Electronics and Instrumentation Engineering at Erode Sengunthar Engineering College, India. Her research areas include Digital Image Processing, Artificial Intelligence, Deep Learning. Also, in addition to this, she had an ISTE membership.

R. Raja Kumar graduated in Mathematics and he completed his doctorate in Chaotic Communications in 2013. He is a Professor of Mathematics in Sathyabama Institute of Science and Technology (Deemed University), Chennai, Tamil Nadu, India. He has 30 years of teaching experience and has 50 reputed publications and 6 International books to his credit. He is a member of Ramanujan Mathematical Society. His research interests include Communication Engineering and Mathematics.

Arrived: 05.08.2023
Accepted: 15.10.2023