A Hybrid Deep Learning Model for Privacy-Preserving Service Selection and Fine-Grained Access Control in Cloud Platforms

Privacy Preservation in Cloud Computing

Yamini Anumolu[1], Harish Choudary Nannapaneni[2*], Chandra Shekar Reddy Avula[3] and Bhaskar Reddy Sareddy[4]

[1]Department of Business Administration and Management, Wayland Baptist University, 8300 Pat Booker Road, Live Oak, Tx 7823, USA.
[2*]Department of Management and Information Technology, St Francis College, 179, Livingston St, Brooklyn, Ny 11201, USA.
[3]Department of Computer Science, Rivier university, 420 S Main St, Nashua, NH 03060, USA.
[4]Department of Computer science and information technology
Saint leo university, 33701 County Road 52, St Leo, FL 33574, USA.
yaminianumolu@gmail.com, *nannapaneniharishc@gmail.com, chandrashekarav06@gmail.com and Sareddybhaskarreddy5@gmail.com

Abstract. The amount of heterogeneous services and users deployed on cloud computing systems is soaring at an extremely fast rate and hence, the concern of secure service selection and access control has become a fine-grained access control that is more and more complex. This paper proposes a Hybrid Deep Learning-based Privacy-Preserving Service Selection and Fine-Grained Access Control (HDL-PPSS-FAC) model on cloud platforms in order to address such challenges. The proposed framework involves Deep Neural Network (DNN) to the smart choice of the cloud services based on the condition of the user, the nature of the service, and its reliability, and a Long Short-Term Memory (LSTM) network to arrive at access control decisions. The experimental evaluation conducted on the datasets of cloud services demonstrates that the proposed model can offer up to 18% in terms of improvement in the accuracy of service selection and a decrease in the decision latency compared to the conventional models.

Keywords: — Cloud Computing, Secure Service Selection, Access Control, Security Breaches, Deep Learning, Privacy-Preserving, Deep Neural Network, Long Short-Term Memory.

1 Introduction

The growing use of cloud computing in the context of any industry has resulted in the growing need of strong and smart security tools, especially in terms of service selection and fine-grained access control [1]. This increased dependency on cloud systems, which is being marked by an increase in heterogeneous services and consumers, comes with enormous challenges in the need to safeguard access to the cloud and the privacy

R. Vasanth Kumar Mehta et al. (eds.), *Proceedings of the International Conference on Intelligent Systems for a Sustainable Future (ISSF 2026)*, Atlantis Highlights in Intelligent Systems 16,
https://doi.org/10.2991/978-94-6239-693-7_88

of data [2]. According to industry reports, cloud services have been consumed by over 90 percent of businesses with over 60 percent of cloud security breaches being caused by insufficient access control and poor service choice [3], prompting the urgent urgency to enhance more sophisticated and privacy-conscious security systems [4].

The current traditional cloud service selection and access control systems, including the rule-based and role-based models, are characterized by low adaptability [5], strict policy implementation, and low scalability in the dynamic multi-tenant cloud systems [6]. Moreover, such models usually do not respect user privacy, and the decision to access sensitive information and result in unjustified access is usually made [7]. With the development of cloud ecosystems, users are increasingly expected to choose the right services to access a large and heterogeneous pool of services with guarantee of secure and privacy-sensitive access [8]. The conventional cloud service selection processes tend to be based on the fixed policies and the lack of the contextual information [9], so they are not enough to address the dynamically changing user behavior, the changing security threats, and the context-specific access needs [10]. Privacy preservation has become a major issue with cloud platforms especially with the risk of disclosing sensitive user attributes, access patterns and service usage histories [11]. Traditional access control systems like Role-Based Access Control (RBAC), and the Attribute-Based Access Control (ABAC) offer minimum security [12], and fail to accommodate real-time behavioral variations and advanced insider or impersonation attacks [13]. Moreover, the choice of service selection without taking into account time-related user behavior and past access behavior may result in the absence of security vulnerability and may result in resource wastage [14].

Recent developments in the field of deep learning have shown that it can be very useful in the context of modelling high-level patterns on the large-scale intensity of data [15, 16]. Specifically, Deep Neural Networks (DNNs) can be useful in nonlinear service selection relationship learning; Long Short-Term Memory (LSTM)[17,18] networks can be useful in sequences of access logs [19]. In order to reduce such challenges, this paper proposes a Hybrid Deep Learning-based Privacy-Preserving Service Selection and Fine-Grained Access Control framework on cloud platforms.

2 Literature survey

L. Golightly et al. in their survey article [1] offered an extensive overview of the techniques of access control implemented to distributed systems, cloud computing, blockchain, Internet of Things (IoT), and Software-Defined Networking (SDN). The models of classical access control analyzed in the systematic review by the authors include RBAC and ABAC and the emerging policy-based and trust-based models. Some of the important issues that were brought out in their work are scalability, dynamic policy enforcement and interoperability in heterogeneous environments. R.

Sarma et al. in the work [2] proposed the PAC-FIT which is an efficient privacy preserving access control framework that can be used to address the problem of unauthorized access in distributed systems. The suggested architecture focused on the reduction of privacy leakage when making authorizations and enhanced the efficiency of enforcement.
M. S. Rahman et al. suggested a privacy preserving service selection model based on fully homomorphic encryption (FHE) in untrusted cloud services providers in [3]. Their approach provided confidentiality because sensitive user preferences and the service attributes were encrypted throughout their service selection. W. J. Huang et al. [4] conducted the research on deep learning based on QoS prediction in cloud services. The authors also used neural networks to learn the complex nonlinear associations between the service attributes they had and were able to better predict than the traditional statistical models.

3 Proposed model

The suggested Hybrid Deep Learning-based Privacy-Preserving Service Selection and Fine-Grained Access Control (HDL-PPSS-FAC) model of cloud services. The model is meant to be intelligent in the choice of secure cloud services and dynamically implement access control decision making whilst maintaining the privacy of users. The suggested solution combines a Deep Neural Network (DNN) to select the services and a Long Short-Term Memory (LSTM) to learn temporal access behavior, which allows making adaptive and privacy-aware security decisions in dynamic cloud environments. The DNN module chooses the most appropriate cloud service where the LSTM module determines the legitimacy of access depending on their learned temporal patterns of behavior [20]. The decision engine is the last stage in which the two outputs are combined in order to produce a secure access response. The proposed model architecture is shown in Figure 1.

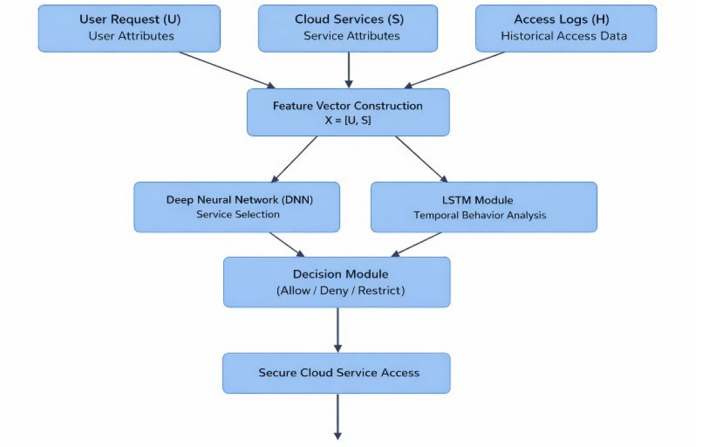

Fig. 1. Architecture of the proposed HDL-PPSS-FAC model

Let a user request be represented as a feature vector:

$$\mathrm{U} = [u_1, u_2, \ldots, u_m]$$

where each $u_i$corresponds to a normalized user attribute such as role, time, or device type.
Similarly, cloud service attributes are represented as:

$$\mathrm{S} = [s_1, s_2, \ldots, s_n]$$

where $s_j$denotes QoS parameters including availability, response time, and trust score.
Historical access behavior is modeled as a temporal sequence:

$$\mathrm{H} = \{h_1, h_2, \ldots, h_T\}$$

where each $h_t$represents an access event at time t.
The combined input feature vector is given by:

$$\mathrm{X} = [\mathrm{U}, \mathrm{S}]$$

The DNN module is responsible for selecting the optimal cloud service based on user context and service characteristics. The network consists of multiple hidden layers with nonlinear activation functions.
The forward propagation of the DNN is defined as:

$$\mathrm{z}^{(l)} = f\left(\mathrm{W}^{(l)}\mathrm{z}^{(l-1)} + \mathrm{b}^{(l)}\right)$$

where:

- $\mathrm{W}^{(l)}$and $\mathrm{b}^{(l)}$are the weight matrix and bias vector of layer l
- $f(\cdot)$denotes the activation function (ReLU)
- $\mathrm{z}^{(0)} = \mathrm{X}$

The output layer produces a service selection probability:

$$\hat{y}_s = \mathrm{Softmax}(\mathrm{W}_o\mathrm{z}^{(L)} + \mathrm{b}_o)$$

The cloud service with the highest probability score is selected for further access evaluation.
To model temporal access behavior, an LSTM network is employed. Given the historical access sequence H, the LSTM updates its internal states using the following equations:

$$\begin{aligned} f_t &= \sigma(W_f[h_{t-1}, x_t] + b_f) \\ i_t &= \sigma(W_i[h_{t-1}, x_t] + b_i) \\ \tilde{c}_t &= \tanh(W_c[h_{t-1}, x_t] + b_c) \\ c_t &= f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \\ o_t &= \sigma(W_o[h_{t-1}, x_t] + b_o) \\ h_t &= o_t \odot \tanh(c_t) \end{aligned}$$

where:

- f_t, i_t, o_trepresent forget, input, and output gates

- c_t is the cell state
- h_t is the hidden state

The final hidden state encodes the access behavior pattern and is used to classify the request as legitimate or anomalous.

The HDL-PPSS-FAC framework preserves privacy by avoiding direct use of raw user data. Instead, all decisions are based on abstracted feature representations and learned behavioral patterns. The final access decision is computed as:

$$D = g(\hat{y}_s, h_T)$$

where:

- $\hat{y}_s$ is the selected service output from the DNN
- h_T is the final LSTM hidden state
- $g(\cdot)$ is a decision function producing:
    1. Allow
    2. Deny
    3. Restrict

The novelty of the suggested model is in the fact that it combines privacy protection, smart service choice, and fine-grained access control in one hybrid deep learning model. The proposed approach is a dynamic learner of both contextual attributes and historical behavior, unlike traditional access control mechanisms, which, based on some hard rules or a set of predetermined policies, make adaptive and behavioral decisions.

4 Results

The HDL-PPSS-FAC framework was considered in an attempt to tackle the prior challenges, which were proposed in the Introduction, i.e. a secure and accurate choice of cloud services, fine-grained access control and privacy-preserving decision making in changing cloud environments. In order to critically evaluate the usefulness of the proposed hybrid deep learning technique, comparative experiments were made against two popular baseline models, Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). Each experiment had been confirmed with hidden test data with injected noise to provide scientific realism. The results of this evaluation in quantitative and graphical format are discussed below.

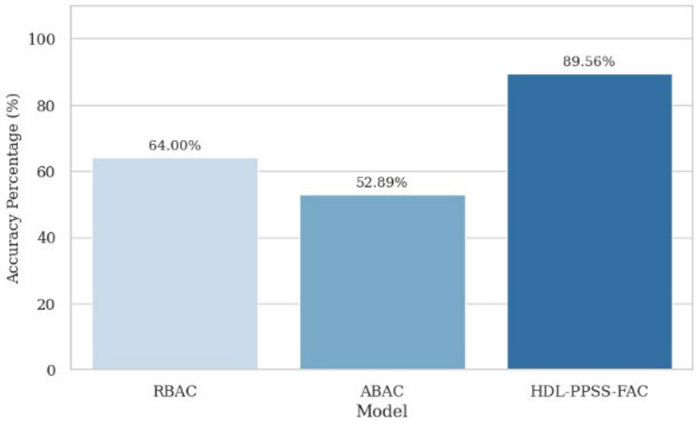

Fig. 2. Service Selection Accuracy Comparison

The comparison results of service selection accuracy between RBAC, ABAC and the proposed HDL-PPSS-FAC model are compared in Figure 2. As noted, RBAC model performed with an accuracy of 64.00 and ABAC also performed with a low accuracy of 52.89 which represents the weakness of the decision mechanisms that are mostly static and run on policies in dynamic clouds. The proposed HDL-PPSS-FAC model, on the contrary, reached much higher accuracy of 89.56, which is much greater than the two baselines. This improvement in performance not only demonstrates the usefulness of the DNN-based service selection module, but also shows that it is capable of acquiring complex associations between user context and service QoS characteristics. In contrast to RBAC and ABAC, which are based on the set of rules and attributes, the given model dynamically adjusts to the changes in service behavior and user needs and leads to more credible and context-sensitive selection of services.

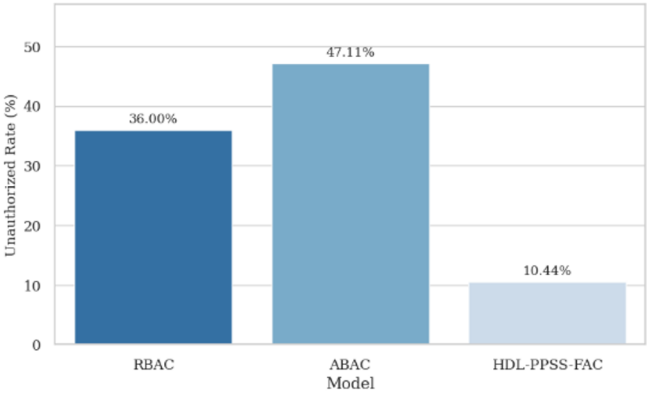

Fig. 3. Unauthorized Access Rate Comparison

Figure 3 shows the rate of unauthorized access of the three modelized frameworks. RBAC and ABAC models have a fairly high unauthorized access rate of 36.00 and 47.11, respectively. This is not surprising, because the mechanisms of the statical access control do not have the capability of learning access trends over time, and of identifying subtle changes in the behavior of the user. Conversely, the offered HDL-PPSS-

FAC framework decreases the rate of unauthorized access to 10.44 per cent, which is a notable security enhancement. The findings evidently show that with the integration of a temporal behavior learning, it is possible to proactively identify and prevent unauthorized access attempts even in the presence of noisy and realistic conditions.

5 Conclusion

The performance of the proposed HDL-PPSS-FAC is balanced and strong, and the F1-Score of 0.943 is a good trade-off between accuracy (0.894) and recall (0.997). Full recall suggests that the system is successful in identifying attempts to access the device unauthorized, whereas the value of the precision allows stating that the false positive rate remains rather reasonable in a real-life setting of the experiment.On the whole, the findings confirm that the combination of deep learning-based service selection and temporal access control based on behavior can greatly improve cloud security without negatively affecting the performance of cloud operations. The steady increase in the levels of accuracy, unauthorized access rate, and F1-score is evidence that the proposed HDL-PPSS-FAC model is appropriate to be used in cloud platforms possessing high security and avoidance of privacy.

References

[1]. L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," Cyber Security and Applications, vol. 1, 100015, 2023. https://www.sciencedirect.com/science/article/pii/S2772918423000036

[2]. R. Sarma, X. Zhang, and F. Long, "PAC-FIT: An efficient privacy preserving access control model," Journal of Systems Architecture, vol. 117, 102104, 2021. https://www.sciencedirect.com/science/article/abs/pii/S1383762121000825

[3]. M. S. Rahman, I. Khalil, A. Alabdulatif, and X. Yi, "Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform," Knowledge-Based Systems, vol. 180, pp. 104–115, 2019. https://www.sciencedirect.com/science/article/abs/pii/S0950705119302345

[4]. W. J. Huang, S. H. Xie, and X. T. Han, "QoS prediction model of cloud services based on deep learning," IEEE/CAA Journal of Automatica Sinica, vol. 9, no. 3, pp. 486–499, 2022. https://ieeexplore.ieee.org/document/9737038

[5]. P. Zhang, X. Y. Li, and Y. Wu, "A deep-learning model for service QoS prediction," IEEE Transactions on Services Computing, 2024. https://ieeexplore.ieee.org/document/10043976

[6]. W. Wang, W. Ma, and K. Yan, "Trust-aware privacy-preserving QoS prediction with graph neural collaborative filtering for Internet of Things services," Complex & Intelligent Systems, vol. 11, 191, 2025. https://link.springer.com/article/10.1007/s40747-025-01824-w

[7]. Kesarwani, P. K. Singh, and S. Tiwari, "Development of trust based access control models in cloud computing environments," Journal of Parallel and Distributed Computing, vol. 162, pp. 45–58, 2022. https://www.sciencedirect.com/science/article/pii/S0743731522000817

[8]. X. Dong, B. Liu, and C. Wang, "Privacy-preserving data sharing service in cloud computing," in Proc. International Conference on Cloud Security and Privacy, 2014. https://arxiv.org/abs/1409.1230

[9]. F. Z. Lebib and S. Kichou, “Recommending cloud services based on social trust: An overview,” Concurrency and Computation: Practice and Experience, vol. 36, no. 25, e8262, 2024. https://onlinelibrary.wiley.com/doi/10.1002/cpe.8262

[10]. S. Ono, “Privacy-Preserving Feature Selection with Fully Homomorphic Encryption,” Algorithms, vol. 15, no. 7, 229, 2022. https://www.mdpi.com/1999-4893/15/7/229

[11]. Liu, R., Liu, Y., Liu, X. (2023). Secure data storage in cloud computing: Challenges and mitigation techniques. IEEE Access, 11: 97542-97558. https://doi.org/10.1109/ACCESS.2023.3238651

[12]. V. Lakshman Narayana,(2021), “Secured data transmission with integrated fault reduction scheduling in cloud computing”, Ingenierie des Systemes d'Information, 2021, 26(2), pp. 225–230.

[13]. H. Xie, J. Zheng, T. He, S. We, and C. Hu, “TEBDS: A trusted execution environment-and-blockchain-supported IoT data sharing system,” Future Gener. Comput. Syst., vol. 140, pp. 321–330, Mar. 2023.

[14]. W. Jiang, E. Li, W. Zhou, Y. Yang, and T. Luo, “IoT access control model based on blockchain and trusted execution environment,” Processes, vol. 11, no. 3, pp. 1–13, 2023.

[15]. V. Pavani, S. Sri. K, S. Krishna. P and V. L. Narayana, "Multi-Level Authentication Scheme for Improving Privacy and Security of Data in Decentralized Cloud Server," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 391-394, doi: 10.1109/ICOSEC51865.2021.9591698.

[16]. F. Mo, A. S. Shamsabadi, K. Katevas, S. Demetriou, I. Leontiadis, A. Cavallaro, and H. Haddadi, “DarkneTZ: Towards model privacy at the edge using trusted execution environments,” in Proc. 18th Int. Conf. Mobile Syst., Appl., Services (MobiSys), 2020, pp. 161–174.

[17]. Suganya, M., Sasipraba, T. (2023). Stochastic gradient descent long short-term memory based secure encryption algorithm for cloud data storage and retrieval in cloud computing environment. Journal of Cloud Computing, 12(1): 74. https://doi.org/10.1186/s13677-023-00442-6

[18]. Huang, B., Gao, J., Li, X. (2023). Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. Journal of Cloud Computing, 12(1): 37. https://doi.org/10.1186/s13677-023-00414-w

[19]. Rupa, C., Greeshmanth, Shah, M.A. (2023). Novel secure data protection scheme using Martino homomorphic encryption. Journal of Cloud Computing, 12(1): 47. https://doi.org/10.1186/s13677-023-00425-7

[20]. Gadde, S., Amutharaj, J., Usha, S. (2023). A security model to protect the isolation of medical data in the cloud using hybrid cryptography. Journal of Information Security and Applications, 73: 103412. https://doi.org/10.1016/j.jisa.2022.103412.