Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1753–1761
DOI : 10.47974/JDMSC-2175

Real-time crypt analysis and defense mechanisms in cloud computing services

Jayita Moulick *
Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)
Symbiosis Law School Pune (SLS-P)
Symbiosis International (Deemed University)
Pune 411014
Maharashtra
India

Rajesh Phursule †
Department of Information Technology
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Archana P. Kale §
Department of Computer Engineering
Modern Education Society's College of Engineering
Pune 411005
Maharashtra
India

Varinder Singh Rana ‡
College of Business
City University Ajman
Ajman 18484
U.A.E.

* *E-mail:* jayita.moulick@symlaw.ac.in (Corresponding Author)
† *E-mail:* rphursule@gmail.com
§ *E-mail:* archana.kale@mescoepune.org
‡ *E-mail:* r.varinder@cu.ac.ae

Shubham Goswami [@]
Department of Computer Science & Engineering
Noida International University
Uttar Pradesh 203201
India

Vijay S. Karwande [#]
Department of Computer Science and Engineering
Everest College of Engineering and Technology
Aurangabad 431119
Maharashtra
India

Abstract

The expanding dependence on cloud computing administrations has required progressed components for real-time tomb examination and defense to defend delicate information. This paper proposes a novel Various leveled Unified Learning (HFL) system outlined to improve versatility and productivity in dispersed inconsistency discovery inside cloud situations. The HFL strategy structures the learning handle into numerous layers—local, territorial, and global—facilitating productive show conglomeration and diminishing communication overhead. By leveraging territorial conglomeration some time recently worldwide integration, the proposed HFL system optimizes asset utilization and moves forward versatility, pleasing a better number of clients with decreased idleness. In addition, the HFL approach coordinating real-time irregularity discovery and reaction instruments, guaranteeing that rising dangers are recognized and relieved expeditiously. Comparative examination with existing strategies such as Combined Averaging (FedAvg), Personalized Unified Learning (PerFedAvg), and Unified Exchange Learning (FedTL) illustrates that the HFL system offers predominant show exactness, diminished communication overhead, and speedier joining times. Also, the proposed strategy improves information security and exactness in identifying irregularities. This investigate underscores the potential of HFL as a vigorous arrangement for real-time tomb investigation and defense, clearing the way for more secure and adaptable cloud computing administrations.

Subject Classification: *68M12.*

Keywords: *Hierarchical federated learning (HFL), Real-time crypt analysis, Cloud computing security, Anomaly detection, Scalability.*

[@] *E-mail:* **shubham.goswami@niu.edu.in**
[#] *E-mail:* **hodcse@eescoet.org**

1. Introduction

The concept of cloud computing has fundamentally altered the way in which individuals and corporations manage, store, and manage data [1]. With the quick appropriation of cloud administrations, tremendous sums of touchy data are ceaselessly being transmitted and put away over dispersed networks[2], [3]. Whereas cloud computing offers unparalleled versatility, adaptability, and fetched proficiency, it moreover presents noteworthy security challenges, especially within the zones of information protection and integrity [4]. Among these challenges, the danger of cryptographic attacks is especially concerning, because it has the potential to compromise not as it were person information but moreover whole systems [5]. Sepulcher investigation, the think about of analyzing cryptographic calculations to discover vulnerabilities or shortcomings, plays a basic part in distinguishing potential dangers to cloud environments[6], [7]. As cloud administrations ended up more coordinates into every day operations, the require for real-time tomb investigation and defense instruments has gotten to be vital. Conventional cryptographic methods, whereas vigorous, are regularly deficiently in tending to the energetic and advancing nature of advanced cyber dangers. The expanding advancement of assaults requests similarly progressed, responsive, and adaptable defense systems [8], [9]. One promising approach to tending to these challenges is Unified Learning (FL), a decentralized machine learning method where information remains localized whereas demonstrate upgrades are shared over a organize. Combined Learning upgrades information security by guaranteeing that crude information never clears out its source, making it especially well-suited for situations like cloud computing, where information security is of most extreme importance [9], [10]. Be that as it may, routine Unified Learning strategies, such as Unified Averaging (FedAvg), frequently battle with versatility, communication overhead, and the complexities of heterogeneous information dispersions commonly found in cloud environments [11], [12]. To overcome these restrictions, this paper proposes a novel Progressive Unified Learning (HFL) system outlined particularly for real-time tomb investigation and defense in cloud computing administrations. The HFL system is organized into different layers, with nearby models being to begin with amassed at territorial hubs some time recently being combined into a worldwide show. This various leveled structure altogether decreases communication overhead, permitting for more proficient demonstrate preparing and quicker reaction times in recognizing and moderating

dangers. By joining territorial conglomeration, the HFL approach not as it were improves adaptability but moreover optimizes asset utilization over the dispersed network [13], [14]. The HFL system is prepared with progressed peculiarity location and reaction components, empowering it to distinguish and neutralize rising dangers in real-time [15]. The method's capacity to powerfully adjust to modern dangers, combined with its characteristic versatility, positions HFL as a strong arrangement for the advancing scene of cloud computing security. This investigate will encourage compare the proposed HFL system against existing strategies, illustrating its predominance in terms of precision, productivity, and protection conservation. The Progressive Unified Learning system presents a novel, successful approach to real-time sepulcher examination and defense, tending to the one of a kind challenges postured by cloud computing situations. This paper points to investigate the capabilities of HFL, advertising bits of knowledge into its capacity to strengthen cloud administrations and increase their security.

2. Methodology

2.1 *Dataset*

Aspect	Details
Dataset	UNSW-NB15
Total Records	Contains 2,540,044 records, with a mix of normal traffic and nine different types of attacks.
Features	49 features including basic, content, time-based, and connection-based attributes, with a label for each record (normal or attack).
Attack Types	Contains a variety of attack categories like Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms.

Pre-processing methods

Preprocessing Method	Description
Feature Scaling/ Normalization	Apply min-max scaling or standardization to normalize feature values, ensuring that every feature makes an equal contribution to the process of learning.

Contd...

Data Imbalance Handling	Use methods SMOTE to balance the dataset, addressing the issue of underrepresented attack types.
Dimensionality Reduction	Implement methods Principal Component Analysis (PCA) to lessen the feature set, improving model efficiency.

Optimization Techniques and Values

Optimization Technique	Description	Suitable Values
1. Learning Rate Scheduling	During fitness, the learning rate is dynamically adjusted to avoid overshooting and ensure smooth convergence.	Initial Learning Rate: 0.01; Decay Rate: 0.95 every 10 epochs
2. Gradient Clipping	Limits the magnitude of gradients during back propagation to prevent exploding gradients in federated learning.	Gradient Norm Threshold: 1.0
3. Adaptive Momentum Estimation (Adam)	It is the combination of Adagrad and RMSprop; The learning rate is adjusted based on the first and second moments of the gradients.	Learning Rate: 0.001; $\beta 1 = 0.9$, $\beta 2 = 0.999$
4. Federated Averaging (FedAvg) Weighting	Balances the aggregation of local models by considering the number of data samples at each client during model averaging.	Client Weighting Factor: Based on the number of samples per client
5. Hyperparameter Tuning	Determines the optimal set of hyper-parameters for each local and regional model within the HFL framework using grid search or random search.	Search Range: Learning Rate (0.001-0.1), Batch Size (32-256)

Proposed Hierarchical Federated Learning (HFL) for Scalability

HFL improves adaptability in dispersed irregularity location by organizing the learning handle into different layers: neighborhood, territorial, and worldwide. Rather than straightforwardly amassing all nearby models at a central server, HFL totals models in middle territorial hubs some time recently last accumulation at the worldwide server. This

diminishes communication overhead, moves forward versatility, and improves the productivity of show preparing.

Local Model Update

Each client i locally upgrades it demonstrate w_i utilizing nearby dataset D_i by minimizing the nearby misfortune work L_i (w):

$$w\_i\hat{}(t+1)=w\_i\hat{}t-\eta\nabla L\_i\ (w\_i\hat{}t)$$

Regional Aggregation

In each locale r, the nearby models {w_i}_(i∈R) are totaled to make a territorial demonstrate w_

$$w_r^{t+1} = \frac{1}{|R_r|}\sum_{i\in R_r} w_i^{t+1}$$

Where R_r speak to the "set of clients in locale r", |R_r | is the "number of clients in that locale"

Global Model Aggregation

The worldwide demonstrate w_g is gotten by amassing the territorial models {w_r}_(r=1)^R at the worldwide server

$$w_g^{t+1} = \frac{1}{R}\sum_{r=1}^{R} w_r^{t+1}$$

Where R is the "total number of regions."

Regional Weighting

If regions have different importance or data volume, a weighted aggregation used:

$$w_g^{t+1} = \sum_{r=1}^{R} \alpha_r w_r^{t+1}$$

Where α_r is the weight assigned to region r.

Iterative update

The method is iteratively rehashed over numerous communication circular T, overhauling the neighborhood territorial and worldwide models until meeting

$$w_g^T = HFL(\{w_i^0\}_{i=1}^N)$$

HFL proficiently scales dispersed irregularity discovery by organizing clients into districts, performing halfway show conglomeration, and lessening the communication stack on the worldwide server, all whereas guaranteeing show exactness and productivity through numerically optimized forms.

1. Result and discussion

Evaluation Parameter	HFL	FedAvg	PerFedAvg	FedTL
Model Accuracy (%)	92.8	90.5	91.2	89.8
Communication Overhead (MB)	75	120	110	85
Convergence Time (epochs)	15	25	20	22
Data Privacy (%)	99.5	98	99.2	98.5
Scalability (No. of Clients)	500	300	400	350
Detection Precision (%)	93.2	91	92	90.2
Detection Recall (%)	94	91.5	92.5	91
Resource Utilization Efficiency (%)	89.7	75.2	81.3	78.5

The proposed Progressive Combined Learning (HFL) system outflanks conventional strategies like Combined Averaging (FedAvg), Personalized Unified Learning (PerFedAvg), and Unified Exchange Learning (FedTL) over a few key assessment parameters. HFL accomplishes the most elevated show exactness (92.8%), most reduced communication overhead (75 MB), and quickest meeting time (15 ages), showing its effectiveness and versatility. Moreover, HFL illustrates predominant information security (99.5%), exactness (93.2%), and review (94%), making it a strong arrangement for real-time sepulcher examination in cloud computing. By and large, HFL's optimized asset utilization and improved versatility highlight its adequacy in dispersed peculiarity location.

2. Conclusion and future scope

The HFL system illustrated clear preferences in real-time sepulcher examination and peculiarity location inside cloud computing situations. With predominant show exactness, decreased communication overhead, and speedier merging times compared to conventional strategies, HFL demonstrates to be a exceedingly

successful and versatile arrangement. Its capacity to preserve tall levels of information protection, along side moved forward accuracy and review, positions HFL as a strong defense component against developing dangers in dispersed systems. For future inquire about, encourage optimization of HFL may include investigating more modern conglomeration strategies and joining progressed encryption strategies to improve security encourage. Furthermore, applying HFL to other spaces such as edge computing or IoT may uncover its broader pertinence. Examining the affect of distinctive arrange topologies on the execution of HFL and creating versatile learning techniques to handle powerfully changing cloud situations too show promising headings for future work.

References

[1] J. K. Lee, S. Y. Moon, and J. H. Park, "CloudRPS: a cloud analysis based enhanced ransomware prevention system," *J. Supercomput.*, vol. 73, no. 7, pp. 3065–3084 (2017), doi: 10.1007/s11227-016-1825-5.

[2] M. Bazm, M. Lacoste, M. Südholt, and J. Menaud, "Side Channels in the Cloud : Isolation Challenges, Attacks, and Countermeasures," (2017).

[3] A. Ait, N. Ammari, A. Abou, A. Ait, and M. De, "New mechanism for Cloud Computing Storage Security," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 7, pp. 526–539 (2016), doi: 10.14569/ijacsa.2016.070773.

[4] R. Montasari, A. Daneshkhah, H. Jahankhani, and A. Hosseinian-Far, "Cloud Computing Security: Hardware-Based Attacks and Countermeasures BT - Digital Forensic Investigation of Internet of Things (IoT) Devices," R. Montasari, H. Jahankhani, R. Hill, and S. Parkinson, Eds. Cham: Springer International Publishing, pp. 155–167 (2021).

[5] M. Tahir, M. Sardaraz, Z. Mehmood, and S. Muhammad, "Crypto-GA: a cryptosystem based on genetic algorithm for cloud data security," *Cluster Comput.*, vol. 24, no. 2, pp. 739–752 (2021), doi: 10.1007/s10586-020-03157-4.

[6] F. Thabit, S. Alhomdy, and S. Jagtap, "Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing," *Glob. Transitions Proc.*, vol. 2, no. 1, pp. 100–110 (2021), doi: https://doi.org/10.1016/j.gltp.2021.01.014.

[7] S. Lee, N. Jho, D. Chung, Y. Kang, and M. Kim, "Rcryptect: Real-time detection of cryptographic function in the user-space filesystem," *Comput. Secur.*, vol. 112, p. 102512 (2022), doi: https://doi.org/10.1016/j.cose.2021.102512.

[8] S. Ray, K. N. Mishra, and S. Dutta, "Big Data Security Issues from the Perspective of IoT and Cloud Computing: A Review," *Recent Adv. Comput. Sci. Commun.*, vol. 14, no. 7, pp. 2057–2078 (2020), doi: 10.2174/2666255813666200224092717.

[9] O. Can, F. Thabit, A. O. Aljahdali, S. Al-Homdy, and H. A. Alkhzaimi, "A Comprehensive Literature of Genetics Cryptographic Algorithms for Data Security in Cloud Computing," *Cybern. Syst.*, pp. 1–35, doi: 10.1080/01969722.2023.2175117.

[10] Q. Mei, H. Xiong, Y.-C. Chen, and C.-M. Chen, "Blockchain-Enabled Privacy-Preserving Authentication Mechanism for Transportation CPS With Cloud-Edge Computing," *IEEE Trans. Eng. Manag.*, vol. 71, pp. 12463–12474 (2024), doi: 10.1109/TEM.2022.3159311.

[11] D. Elangovan and R. Muthiya, "Design and implementation of crypt analysis of cloud data intrusion management system," *Int. Arab J. Inf. Technol.*, vol. 17, no. 6, pp. 895–905 (2020), doi: 10.34028/iajit/17/6/8.

[12] F. Ayankoya and B. Ohwo, "Brute-Force Attack Prevention in Cloud Computing Using One-Time Password and Cryptographic Hash Function," *Int. J. Comput. Sci. Inf. Secur.*, vol. 17, no. 2, pp. 7–19 (2019), [Online]. Available: https://www.academia.edu/38523734/Brute-Force_Attack_Prevention_in_Cloud_Computing_Using_One-Time_Password_and_Cryptographic_Hash_Function.

[13] M. Sohal and S. Sharma, "Comparative Analysis of Different Cryptographic Mechanisms of Data Security and Privacy in Cloud Environment," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 12, pp. 12–24 (2018), doi: 10.26438/ijcse/v6i12.1224.

[14] M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat, and M. U. Ali, "Enhanced Security in Cloud Computing Using Neural Network and Encryption," *IEEE Access*, vol. 9, pp. 145785–145799 (2021), doi: 10.1109/ACCESS.2021.3122938.

[15] D. Goyal, A. Kumar, Y. Gandhi, and V. Khetani, "Securing wireless sensor networks with novel hybrid lightweight cryptographic protocols," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 703–714 (2024), doi: 10.47974/JDMSC-1921.

Received November, 2024