How to Cite:
Venkata, R. G. N., Kalavathi, B. N., Pompapathi, M., Kharb, L., Kumar, V. K., & Selvameena, R. (2022). Privacy enhanced key management protocol for handling remote data using deep learning and evolutionary models. *International Journal of Health Sciences*, *6*(S5), 12353–12360. https://doi.org/10.53730/ijhs.v6nS5.11381

Privacy enhanced key management protocol for handling remote data using deep learning and evolutionary models

Dr. Venkata Ramana Gupta N.
Department of CSE, Assistant Professor, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India,
Email: nallagattla@gmail.com

B. N. Kalavathi
Department of Computer Science, Assistant Professor, Dravidian University, Kuppam, Andhra Pradesh, India,
Email: Kala.kala284@gmail.com

Dr. M. Pompapathi
Information Technology, Associate Professor, RVR & JC College of Engineering, GUNTUR, Andhra Pradesh, India,
Email: manasani.pompapathi@gmail.com

Dr. Latika Kharb
Department of Information Technology, Professor, Jagan Institute of Management Studies, Sector-5, Rohini Delhi-110085
Email: latika.kharb@jimsindia.org

Dr. V. Kiran Kumar
Department of Computer Science, Professor, Dravidian University, Kuppam, Andhra Pradesh, India
Email: kirankumar.v@rediffmail.com.

R. Selvameena
Assistant Professor, Department of Computer Science and Engineering, Dr.M.G.R Educational and Research Institute, Maduravoyal, Chennai-600095
Email: rselvameena1989@gmail.com

***Abstract*---**AI is becoming more common because of expert automated systems and modern technology's ability to process information. This makes our lives easier and more exciting. It's better for privacy, reliability, and network resource use if AI inference algorithms run on a smart device rather than in the cloud, so this is how most smart devices use them. For a long time, on-device intelligence has been

Manuscript submitted: 9 May 2022, Manuscript revised: 18 July 2022, Accepted for publication: 27 August 2022

more common [1]. Cloud and big data have become important tools for pooling resources and training equipment data on the device [2]. Using the important technologies, AI spreads and humans become better at their jobs. Basic Communication technology like gesture recognition is based on data and uses ANN (Artificial Neural Network) algorithms to do periodic tracking and 3D hand modelling [3]. It has been used to run multimedia apps as well as handheld devices by gestures. Security in touch-enabled devices is also important because of authenticating users, which is provided by a learned display contact data set and classifier based on the K-means algorithm. AI-based algorithms are also used in industrial applications to combine live tracking, predictive maintenance, virtual support, and ground truth. This is done by using the cloud and AI-based algorithms.

Keywords---Privacy enhanced key, management protocol, deep learning, evolutionary models.

Introduction

AI is becoming more common, but many apps still use 3rd-party cloud servers to process data. This raises concerns about security, lack of control, and the end up paying of upfront costs. For this reason, new methods use edge computing, which means that algorithms and processes are done right on the gadget. This way, the process can be moved from a cloud server to a private server for more analysis. In most AI-enabled tools, data is stored on the device itself, which makes it more secure than if the data was sent to a third-party processing centre. Edge computing, but at the other hand, performs processing just on hardware machine without needing to connect to the network. Instead, data processing takes place near the network edge, where there is no need for network access. As time-sensitive AI technologies like healthcare, home security, and aerospace become more important, edge intelligence has been seen as a way to make them safer.

Several businesses are also using AI edge intelligence to make better decisions and keep their employees safe in their own communities [8]. IoT networks will also have a big impact on automated driving, portfolio management, network analysis, and community safety. Even though the IoT networks connectivity trend can indeed give people more access to unique and modern applications, embracing it without taking into account the risk of information breaches and security issues could well be a big mistake. IoT networks can provide high scalability, effective spectral efficiency, and strategy development in edge AI. These are all possible benefits of these networks. Privacy and security in IoT networks are becoming more important, even though there are many benefits. The seamless connection and limited resources of data-driven apps make these issues more important. As a result, innovative data confidentiality for a protected edge computing beyond the 5G network is supplied in order to achieve the greatest safety in the edge computer system. The proposed system's principal goal is twofold

- First, privacy is preserved by using a Coalesced machine learning approach in which many edge nodes undertake local training, allowing them to learn from the data input without sharing private data.
- A second method is to use an Artificial Immune System-based Intrusion Detection System (IDS), in which the detectors are educated and distributed as agents to the edge nodes. In contrast to centralised IDS in the cloud, it identifies intruders efficiently by utilising less processing load in IDS.
- Preserving privacy for IOT networks utilizing ML and DL techniques

Encryption, decryption, and clustering of confidential information are all components of the suggested technique. Additionally, the proposed scheme was launched by allocating security based on data obtained from wireless networks. The internet provider, or in other words, the cloud server, allocated the security. Thus, the users are able to access information if, and therefore only if, the client key matches the server key. The EM technique was used to cluster the data, and the Attribute-based Asymmetric encryption was used to encode and decode the grouped data.

Clustering

Firstly, data is collected from internet-connected devices, or, in other words, cloud infrastructure. The EM algorithm is used to group similar pieces of gathered information. The EM algorithm is essentially a strategy that uses communicative methodologies to identify a comparable group of responses. As a result, it is used to identify the more satisfactory settings during the expectation or maximisation steps (MS). Es is often used to determine the expectations function for the log-likelihood assessment provided by the variables. Additionally, the maximising step can be utilised to determine the parameters that were employed to increase the assumption allow ratio (E step). Normal distribution is used when two components with different analysis of variance occur. To determine the similarity of each group of statistics, it is necessary to calculate the frequency distributions for every cluster.

E-step:

The e-step is calculated for every document stored on a cloud platform. It is typically not analysed in order to obtain the lowest variance possible, but rather to assess the likelihood of every cluster. Additionally, cluster 'I' should indeed be computed for all D sample points. This facilitates the analysis of incomplete information and determines the model with the highest degree of similarity. The similarity factor could be used to test the extent to which each clustering point is meaningful. The following expression can be used to get the E-step:

$$E_S(Z_{i,j}) = \frac{P(S = S_i)/(\chi = \chi_j)}{\sum_{i=1}^{k} P(S = S_i)/(\chi = \chi)} \qquad \{1\}$$

In equation 1, χ indicates current model.

In coordinated B5G connections with edge technology, the distributed components (throughput, capacity, and computing capabilities) at the network's edge are adequately integrated and managed by AI algorithms. It enables enormous and precise processing by acquiring data at the device's location. By incorporating AI techniques, edge intelligence enhances our understanding of the network infrastructure. However, employing federated machine learning to analyse data and generate greater knowledge from edge nodes throughout factory networks can give quality management for processing multi-dimensional and multi-variety data with minimal human intervention. Federated devices are a form of community-driven machine learning that enables the training of decentralised data on edge devices while maintaining integrity and confidentiality. Additionally, it impedes data disclosure due to external variables and stores data internally within devices, facilitating a dispersed learning method, which is a desirable characteristic for operational automation (Figure 1).

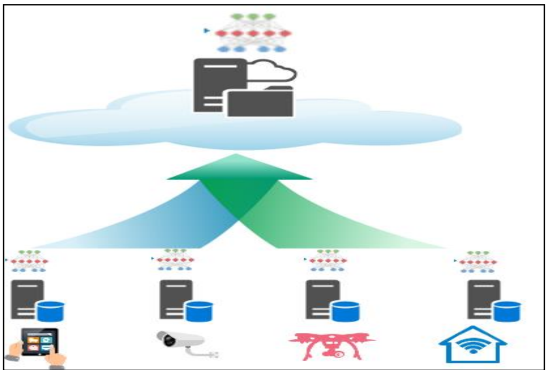

Figure 1. Federated Computer Vision

The overall process of the privacy preservation mechanism[51] using federated machine learning is illustrated in Algorithm .

Algorithm

Privacy preservation using federated machine learning

Input: Local datasets in edge nodes $\text{dataset}_{\text{local}}$, initial global parameters φ_0
Output: global parameters φ
begin
while Central server initiates the global parameters φ_0
Broadcast global parameters φ_0 **do**
while edge nodes capture local gradient $\text{Gradient}_{\text{local}}$ by training the local models Dataseti **do**
Encrypt $\text{Gradient}_{\text{local}} \leftarrow \text{Encrypt}_{\delta}\left(\text{Gradient}_{\text{local}} + \text{laplace}\left(\frac{\Delta GF}{€}\right)\right.$
Form encrypted local gradient values $(\text{Encrypt}_{\text{local}})$
Gross $\text{Encrypt}_{\delta}\left(\sum_{\text{local}=1}^{n} \text{Gradient}_{\text{local}}\right)$
end
while central server grosses encrypted values to edge nodes**do**
$\text{Encrypt}_{\text{global gradient}} \leftarrow \text{Encrypt}_{\delta}\left(\sum_{\text{local}=1}^{n} \text{Gradient}_{\text{local}}\right)$

Determine encrypted text from Encrypt $\text{Gradient}_{\text{local}}$
Generate $\text{Encrypt}_{\text{global gradient}}$
end
while edge nodes decrypts $\text{Encrypt}_{\text{global gradient}}$ to compute $\text{gradient}_{\text{global}}$
$\text{Decrypt}_{\partial}(\text{Encrypt}_{\text{global gradient}}) \leftarrow \sum_{N=1}^{n} \text{Gradient}_{\text{local}}$
Update parameters φ
Aggregate obtained parameters φ to the central server
end

This means that utilizing Paillier Homomorphic Encryption after cryptography concurrently reduces bandwidth consumption and promotes privacy for edge computing architectures. However, the majority of edge computing systems are only semi-trusted, making them vulnerable to a wide range of cybersecurity incidents. There may be a number of effectiveness and performance-related operating costs as a result of the limited resources of the devices. Security across 5G edge of the network therefore necessitates the development of an effective, decentralized warfare approach. Since B5G has a high computational complexity and enormous network traffic, it could be a target for numerous attacks. Throughout the next category, the suggested system contains a unique IDS to protect the network in addition to security and privacy issues in dealing with the challenges.

Experimental Analysis and Evaluation of performance

The performance of the proposed system has been clearly discussed in this section. Various QoS parameters like computational overhead, communication efficiency and accuracy has been analyzed, which helps to determine how performance of proposed system is working. Dataset includes CIFAR-10 and KDD-99 has been utilized to validate the objective function performance.

Accuracy

Accuracy is the considerable QoS performance evaluation metrices which helps to determine the accurate nature of the result. For comparison purposes, we use SVM, Naïve bayes and Random Forest classification algorithm. Equation 6 depicts the accuracy formula,

$$Accuracy = \frac{TP + TN}{sum\ of\ TP, TN, FP, FN} \quad (6)$$

The proposed system has achieved the accuracy of 92.7% for the given epoch of 100, which is better accuracy compared to the existing models. The analyze the performance of accuracy a comparison has to be done with existing approaches. Figure 2 depicts the accuracy comparison of proposed technique with existing approaches.

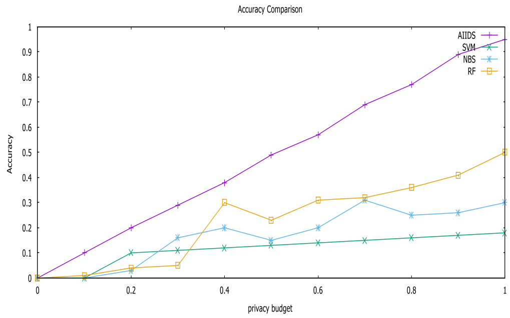

Figure 2. Proposed system accuracy compared with existing approaches

Communication Efficiency

Data transmission frequencies among network edge and cloud servers determines the effective communication. Taking into account both the estimation of local and global gradients is done. Edge users and their appropriate local gradient towards the centralized database and receive the propagated global gradient quantity to update the prototype in each and every encrypted communication. Comparing the efficiency values acquired from the various categorization models is depicted in Figures 10 and 11. Figures 10 and 11 illustrate the graph drawn for a variety of gradients and users, allowing for a more accurate evaluation of the results. Even though the quantity of gradients and users has increased, performance of the model has remained the same. Gradients and the number of users have a significant impact on the communication effectiveness. Proposed models function better than SVM, NBS and RF in efficiency improvements when compared to current models. The implementation of paler encryption, which provides a higher frequency of cypher texts, is indeed the cause of increasing effectiveness.

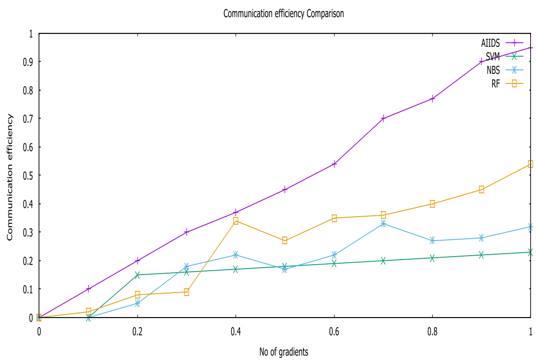

Figure 2. Efficiency of communication on changing quantity of gradients

Conclusion

An edge intelligence approach for IoT Distributed systems is described in the study as a means of preserving safety and confidentiality. The suggested system uses the federated ML model to maintain confidentiality in a collaborative and distributed manner. The Paillier cryptographic algorithm is used to encrypt and decrypt both local and global gradient values, respectively. To ensure that relevant information in the edges nodes is same, it employs different types of attacks. In addition to processing complexity, communication efficiency, performance accuracy, the suggested system beats the standard methods. Different networking attacks have been included to the testing of the remote server and different parameters.

References

1. A. Ahmed and E. Ahmed, "A survey on mobile edge computing," in Intelligent Systems and Control (ISCO), 2016 *10th International Conference on. IEEE*, 2016, pp. 1–8.
2. A. Manzalini and N. Crespi, "An edge operating system enabling anything-as-a-service," *IEEE Communications Magazine*, vol. 54, no. 3, pp. 62–67, 2016.
3. A.M. Rahmani, et al., Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.02.014.
4. Cai, Hongming & Xu, Boyi & Jiang, Lihong & Vasilakos, Athanasios. (2016). IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. *IEEE Internet of Things Journal*. 4. 1-1. 10.1109/JIOT.2016.2619369.
5. D. Conway-Jones, T. Tuor, S. Wang, and K. K. Leung, "Demonstration of federated learning in a resource-constrained networked environment," presented at the *SMARTCOMP IEEE Int. Conf. Smart Comput.*, Jun. 2019.
6. D. Zhu, X. Yang, P. Zhao, and W. Yu, "Towards effective intraflow network coding in software defined wireless mesh networks," in 2015 *24th International Conference on Computer Communication and Networks (ICCCN),* Aug 2015, pp. 1–8.
7. G. Wang, Y. Zhao, J. Huang, and W. Wang, "The controller placement problem in software defined networking: A survey," IEEE Network, vol. 31, no. 5, pp. 21–27, 2017.
8. HA Jalab, HK Omer, Human computer interface using hand gesture recognition based on neural network, *5th National Symposium on Information Technology: Towards New Smart World (NSITNSW),* 2015.
9. J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Trans. Dependable Secure Comput., to be published*, doi: 10.1109/TDSC.2019.2952332.
10. L. Tong, Y. Li, and W. Gao, "A hierarchical edge cloud architecture for mobile computing," in Computer Communications, *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. IEEE*, 2016, Conference Proceedings, pp. 1–9.
11. Li, Youguo & Wu, Haiyan. (2012). A Clustering Method Based on K-Means Algorithm. *Physics Procedia*. 25. 1104-1109. 10.1016/j.phpro.2012.03.206.
12. M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.
13. Manikandan,G. and Anand, M. "Mixed Radix 4 & 8 based SDF-SDC FFT Using MBSLS for Efficient Area Reduction", Indian Journal of Public Health

Research and Development,vol. 9, Issue 10, 2018.(Scopus Indexed, Impact Factor: 0.071).

14. O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the Internet of Things," in Internet of Things (WF-IoT), *2015 IEEE 2nd World Forum on. IEEE*, 2015, Conference Proceedings, pp. 603–608.
15. P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5G on the horizon: key challenges for the radio-access network," IEEE Vehicular Technology Magazine, vol. 8, no. 3, pp. 47–53, 2013.
16. P. Du and A. Nakao, "Application specific mobile edge computing through network softwarization," in Cloud Networking (Cloudnet), 2016 *5th IEEE International Conference on. IEEE, 2016, Conference Proceedings*, pp. 130–135.
17. P. Du and A. Nakao, "Application specific mobile edge computing through network softwarization," in Cloud Networking (Cloudnet), 2016 *5th IEEE International Conference on. IEEE,* 2016, Conference Proceedings, pp. 130–135
18. S Deng, H Zhao, J Yin, S Dustdar, AY Zomaya, Edge Intelligence: The Confluence of Edge Computing and Artificial Intelligence, *IEEE Internet of Things journal*,Volume 7457-7469, 2020.
19. Tim Miller, Explanation in artificial intelligence: Insights from the social sciences, *Artificial Intelligence*, Volume 267, February 2019, Pages 1-38.
20. U. Majeed and C. S. Hong, "FLchain: Federated learning via MECenabled blockchain network," presented at the *APNOMS 20th Asia–Pacific Netw. Oper. Manage. Symp.*, Sep. 2019.
21. W. Yu, H. Xu, H. Zhang, D. Griffith, and N. Golmie, "Ultra-dense networks: survey of state of the art and future directions," in Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016, pp. 1–10.
22. Wang, Y.; Yang, J.; Guo, X.; Qu, Z. Satellite Edge Computing for the Internet of Things in Aerospace. Sensors 2019, 19, 4375.
23. Y. J. Kim and C. S. Hong, "Blockchain-based node-aware dynamic weighting methods for improving federated learning performance," presented at the *APNOMS 20th Asia–Pacific Netw. Oper. Manage. Symp.*, Sep. 2019.
24. Y. Jararweh, A. Doulat, A. Darabseh, M. Alsmirat, M. Al-Ayyoub, and E. Benkhelifa, "SDMEC: software defined system for mobile edge computing," in *Cloud Engineering Workshop (IC2EW), 2016 IEEE International Conference on. IEEE, 2016, Conference Proceeding*s, pp. 88–93.
25. Y. Jararweh, A. Doulat, O. AlQudah, E. Ahmed, M. Al-Ayyoub, and E. Benkhelifa, "The future of mobile cloud computing: integrating cloudlets and mobile edge computing," *in Telecommunications (ICT), 2016 23rd International Conference on. IEEE, 2016, Conference Proceedings*, pp. 1–5.
26. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Trans. Ind. Inform.,* vol. 16, pp. 4177–4186, Jun. 2020.
27. Zhang, Shaojun & Li, Wei & Wu, Yongwei & Watson, Paul & Zomaya, Albert. (2018). Enabling Edge Intelligence for Activity Recognition in Smart Homes. 228-236. 10.1109/MASS.2018.00044.