A Deep Learning Based Privacy Preservation Mechanism for IoT and IoMT Applications

Neelima Singh
VITM Indore

Abstract- *Batch processing in deep learning has been explored extensively to secure IoMT networks. Devices such as Multimedia Sensor Nodes (MSNs) in the IoMT are able to produce both multimedia and non-multimedia data. The generated data are sent from a base station (BS) to a cloud server. However, it's conceivable that the BS and cloud server's Internet connection will be temporarily unavailable. The MSNs are unable to store the acquired data for a prolonged period of time due to the restricted computational capacity. In this case, MSN data can be collected by mobile devices and uploaded to a cloud server. However, this data collection could raise privacy concerns, such as disclosing the identity and whereabouts of MSN users. Thus, when collecting and analyzing such sporadic data from MSNs, it becomes vital to address the issue of data privacy. The article reviews earlier research in the field of privacy-preserving architecture for certain IoMT applications. This paper presents a data collection mechanism and neural batch processing approach for security of IoMT applications. It has been shown that the proposed work attains better performance compared to existing baseline techniques.*

Keywords- Batch Processing, Internet of Multimedia Things (IoMT), Privacy Preservation, IoMT Security

I. INTRODUCTION

The Internet of Multimedia Things (IoMT) refers to the integration of multimedia devices and technologies into the broader Internet of Things (IoT) ecosystem. While the IoT typically focuses on connecting and communicating with various smart devices, IoMT expands this concept to include multimedia devices such as cameras, displays, speakers, and other audiovisual equipment [1]. With IoMT, these multimedia devices become interconnected and capable of capturing, transmitting, and sharing multimedia content over the internet. This integration opens up new possibilities for applications and services that involve multimedia data. Some of the major areas include [3]- [4]::

Smart Surveillance Systems: IoMT enables the deployment of intelligent surveillance systems with connected cameras that can capture and analyze video data in real-time. These systems can detect anomalies, perform facial recognition, and provide enhanced security measures. Interactive Digital Signage: IoMT allows for interactive digital signage that can display multimedia content and respond to user interactions. For instance, a digital sign may use cameras to detect the presence of people and display targeted advertisements or provide information based on the demographics of the audience. Smart Home Entertainment: IoMT enables the integration of multimedia devices within smart homes. For example, you can control your TV, sound system, and streaming services through a central hub or a voice-activated assistant. Collaborative Multimedia Environments: IoMT facilitates multimedia collaboration in various scenarios. For instance, in a business setting, teams can use interconnected multimedia devices to share and manipulate content during meetings or presentations. Enhanced Media Streaming: IoMT can optimize media streaming experiences by dynamically adapting content quality based on network conditions and device capabilities. This ensures a smoother and more immersive multimedia streaming experience [5]

However, it's worth noting that the concept of IoMT is still evolving, and its implementation and impact may vary across different industries and applications. The integration of multimedia devices into the IoT ecosystem brings both opportunities and challenges, including data privacy, security concerns, and interoperability issues that need to be addressed for widespread adoption and success. A fusion of IoT, big data, and cloud storage was presented to preserve the privacy of sensory data collected from e-health systems in [6], [7]. In this work, IoT-related group keys are used to authenticate medical nodes and encrypt messages in a batch processing style to minimize the computational time. An advanced framework for opportunistic routing in delay-tolerant networks was proposed in [8]. In this framework, the main focus is to protect the confidentiality of nodes and perform anonymous authentication using a pairwise communication

II. PRIVACY PRESERVATION IN IOMT APPLICATIONS

All Privacy-Preserving Data Collection and Analysis (P2DCA) is an approach that focuses on safeguarding the privacy of individuals' data during the process of data collection and analysis. It aims to balance the need for data-driven insights with the protection of sensitive information. The P2DCA approach typically employs various techniques and strategies to achieve privacy preservation. Here are some common methods used in P2DCA [9]:

Anonymization: Anonymization techniques are applied to remove or encrypt personally identifiable information (PII) from the collected data. This ensures that individuals cannot be directly identified from the dataset [10].

Differential Privacy: Differential privacy involves adding noise or randomness to the collected data to

relevant privacy regulations and best practices to ensure the responsible and ethical handling of data [15].

III. THE SELF ORGANIZING MAP FOR IOMT SECURITY

Batch Processing

Please Batch Processing intertwined with machine learning can prove to be an effective model for data collection and analysis for privacy preserved applications. Reviewing learning curves of models during training can be used to diagnose problems with learning, such as an underfit or overfit model, as well as whether the training and validation datasets are suitably representative. There is a trade-off between batch size and the speed and stability of the learning process. The learning rule for the training is [16]:

$$\boldsymbol{w_{n+1}} = \boldsymbol{w} - \eta\nabla\boldsymbol{Q}(\boldsymbol{w})\ \mathbf{(1)}$$

protect individuals' privacy. This technique ensures that

$$w_{n+1} = w - \frac{\eta}{n}\sum_{i=1}^{n} \nabla Q_i(w) \qquad (2)$$

the statistical analysis of the data remains accurate while preventing the identification of specific individuals within the dataset.

Secure Multi-Party Computation (SMPC): SMPC allows multiple parties to perform computations on their respective data without exposing their individual data to Both statistical estimation and machine learning consider the problem of minimizing an objective function that has the form of a sum:

each other. This technique enables collaborative

$$Q(w) = \frac{1}{n}\sum_{i=1}^{n} Q_i(w) \qquad (3)$$

analysis while maintaining privacy [11].

Homomorphic Encryption: Homomorphic encryption allows computations to be performed directly on encrypted data, without the need for decryption. This method enables data analysis without exposing the raw data to unauthorized parties.

Privacy-Preserving Data Aggregation: Instead of collecting and analyzing individual-level data, data aggregation techniques can be employed to summarize and analyze data at a higher level. This helps in preserving privacy while still extracting meaningful insights [12].

Privacy Policies and User Consent: Clear privacy policies should be established, and user consent should be obtained before collecting and analyzing their data. Transparent communication and giving individuals control over their data are crucial aspects of privacy preservation [14].

The P2DCA approach emphasizes the importance of privacy protection at every stage of the data lifecycle, from collection to analysis. By implementing these techniques and strategies, organizations can minimize the risk of privacy breaches while still benefiting from valuable data-driven insights. It's essential to adhere to

η is the step size with which weights change

the parameter **w** that minimizes **Q(x)** is to be estimated.

Each summand function Qi is typically associated with the ith observation in the data set (used for training).

In classical statistics, sum-minimization problems arise in least squares and in maximum-likelihood estimation (for independent observations). The general class of estimators that arise as minimizers of sums are called M-estimators. However, in statistics, it has been long recognized that requiring even local minimization is too restrictive for some problems of maximum- likelihood estimation. Therefore, contemporary statistical theorists often consider stationary points of the likelihood function (or zeros of its derivative, the score function, and other estimating equations).

The sum-minimization problem also arises for empirical risk minimization. In this case, Qi(w) is the value of the loss function at ith example, and Q(w) is the empirical risk. When used to minimize the above function, a standard (or "batch") gradient descent method would perform the iterations [17].

Bootstrapping Neural Networks

PA limitation of single neural network models is that they can lack generalization when applied to a seen dataset i.e. the trained neural network gives good performance on the training data but gives unsatisfactory performance on unseen data which are not used in the training process. In training with regularization, the magnitude of network weights is introduced as a penalty term in the training objective function and unnecessarily large network weights are avoided. In training with early stopping, neural network performance on the testing data is checked during the training process and the training process stops when the neural network prediction errors on the testing dataset. The bootstrapping network is depicted din figure 1.

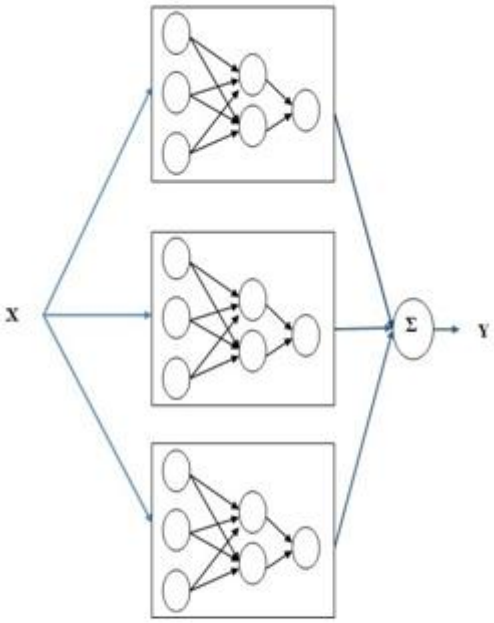

Fig.1: Boostrapping Architecture for Batch Processing

Step.1: Design a simulation of a moderate IoMT network by designing data transmitting/receiving nodes.
Step.2: Design a path loss dependent data transmission model.
Step.3: Assign different attenuation (path loss factors) for different attenuation conditions:

$\alpha = [\alpha_1, \alpha_2, \dots . \alpha_n]$ *(4)*

Here,
$\alpha_1, \alpha_2, \dots . \alpha_n$ ***are the different attenuation constants.***
Step.3: Collect the data from the nodes and feed it to the bootstrapped network based on a training, testing splitting ratio of $\mathbf{70}:\mathbf{30}$
Step.4: Compute the aggregated output as:

Here,

$^{y}agg = \sum^{n} w_i f_i(X)$ *(5)*

y_{agg} ***is the aggregated output.***
f_i ***is the ith aggregated neural network predictor***
w_i ***is the aggregating weight for combining the ith neural network,***
n ***is the number of aggregated neural networks***

Step.5 Compute the cost function for the i th ***predictor as:***
$^{1} n\ b\ 2\ ^{1}$
$^{\sigma}rmse ^{=\{}$
$n\!-\!1$
$\sum_{i=1}[y(x_i w\ ) - y^{(}x_i^{)}]\ \}^2$ *(6)*
Or, σ
$_{=}\ 1$
$\sum^{n} [y(x\ w^b) - y(x\ )]^2$
(7)
mse

$n\!-\!1$
$i\!=\!1\ i\ i$

The bootstrapping architecture is necessary as the amount of data to be analyzed for the IoMT applications is staggeringly large and the data to be analyzed at the could servers or gateways/hubs need to process copious amount of data. While the IoMT data can be of a variety of formats such as text, audio, video etc., yet without any loss of generality, it can be assumed that finally all the data would be sent and received as binary data streams [18].

Proposed Algorithm

The proposed algorithm can be presented as the sequential implementation of the following steps:
Start.
{

Step.6: Evaluate Packet Delivery Ration, Throughput and Communication Overhead as a function of α***.***
Setp.7 Compute Recall, Precision and F-measure.
}
Stop.

IV. EXPERIMENTAL RESULTS

The experimental results of the proposed work have bene evaluated in terms of the performance metrics cited in the proposed algorithm design. For the sake of simplicity, a sector area of 100m x 100m has been used for the purpose of simulation of the IoMT plant. The total iterations to convergence have been chosen as 200 to limit the time complexity of the system.

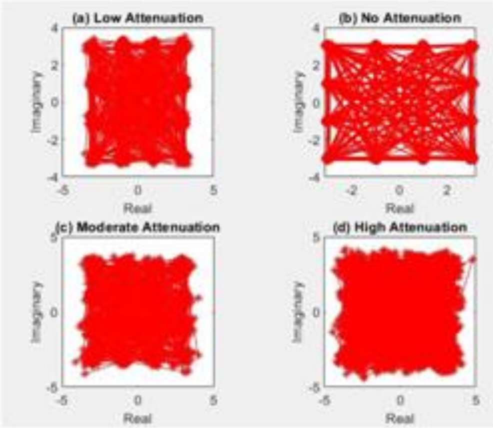

Fig.2: Scatter plot for data packets user different attenuation scenarios

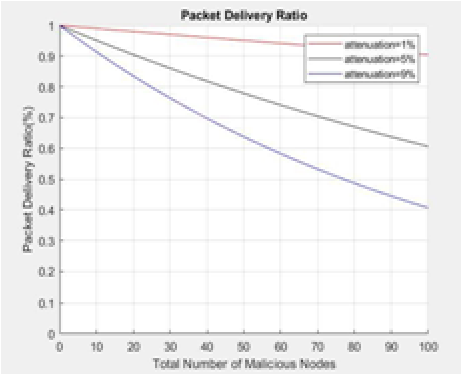

Fig.3: Packet Delivery ratio as a function of malicious nodes

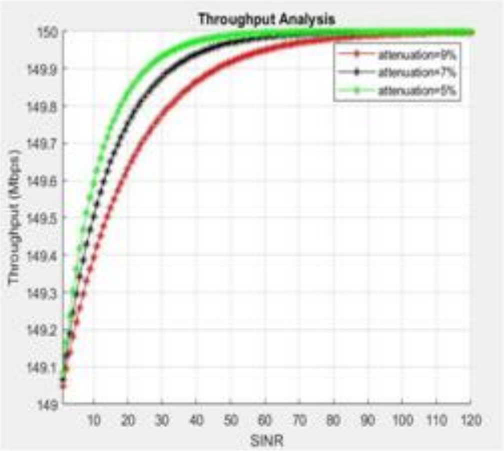

Fig.4: Throughput w.r.t. SINR

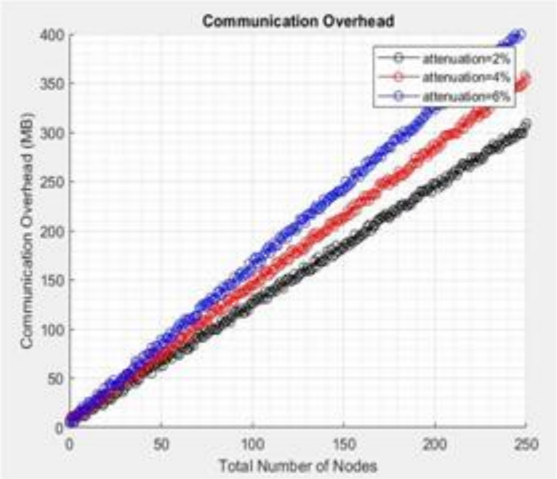

Fig.5: Communication overhead as a funciton of nodes in the network

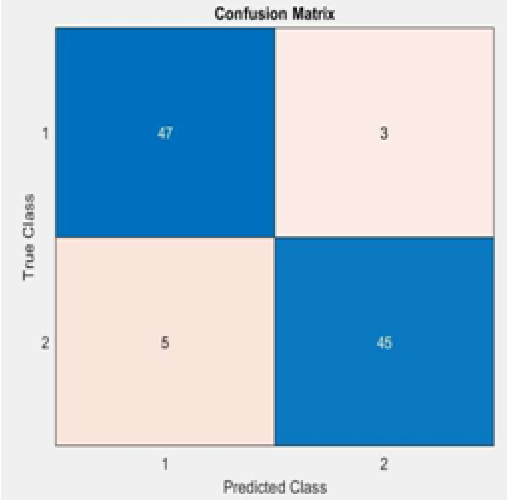

Fig.6: Confusion Matrix

The confusion matrix can be used to compute the Accuracy, Recall, Precision and F-measure of the system, as:

Accuracy: It is defined as:

$$Ac= \frac{TP+TN}{TP+TN+FP+FN} \qquad (8)$$

Recall: It is mathematically defined as:

$$Recall= \frac{TP}{TP+FN} \qquad (9)$$

Precision: It is mathematically defined as:

$$Precisiosn= \frac{TP}{TP+FP} \qquad (10)$$

F-Measure: It is mathematically defined as:

Here.

$$F\text{-}Measure=\frac{2.Precision.Recall}{Precision+Recall} \qquad (11)$$

generating both multimedia and non-multimedia data. The generated data are forwarded to a cloud server viaTP represents true positive TN represents true negative FP represents false positive FN represents false negative

The accuracy is found to be 92%, Recall as 94%, Precision as 90.38% and F-Measure as 91.18%.

A summary of the results obtained from the existing work can be summarized in table 1.

Table 1. Summary of Results

S.No.	**Parameter**	**Value**
1.	Plant Size	100 x 100
2.	Data Stream	Binary
3.	Data Analyzing Model	Bootstrapped Neural Network
4.	Training Method	Batch Processing
5.	Attenuation Model	Low, Moderate, High
6.	Maximum Throughput	15ombps
7.	Maximum Packet Delivery Ratio	90%
8.	Maximum Communication Overhead	400MB
9.	**Precision (Proposed Work)**	**0.9038**
10.	Precision (Previous Work)	0.8784
11.	**Recall (Proposed Work)**	**0.94**
12.	Recall (Previous Work)	0.8151
13.	**F-Measure (Proposed Work)**	**0.9118**
14.	F-Measure (Previous Work)	0.8339

It can be observed from the existing results that the proposed framework employing batch processing attains better performacne in terms of the evaluation metrics with respect to the existing work, compared with. This indicates the higher accuracy of the proposed system and enhanced performance.

V. CONCLUSION

From the previous discussions, it can be concluded that the Multimedia Sensor Nodes (MSNs) are capable of a Base Station (BS). However, it is possible that the Internet connection between the BS and cloud server may be temporarily down. The limited computational resources restrict the MSNs from holding the captured data for a longer time. In this situation, mobile sinks can be utilized to collect data from MSNs and upload to the cloud server. However, this data collection may create privacy issues, e.g., revealing identities and location information of MSNs. To circumvent this issue, a bootstrapped neural network employing batch processing has been proposed which is used as the privacy preserving model for the IoMT applications. It has been shown that the proposed work attains better performance compared to existing baseline techniques.

REFERENCES

[1] M. Usman, M. A. Jan, X. He and J. Chen, "P2DCA: A Privacy-Preserving-Based Data Collection and Analysis Framework for IoMT Applications," in IEEE Journal on Selected Areas in Communications, 2025, vol. 37, no. 6, pp. 1222-1230.

[2] S. Garg, K. Kaur, N. Kumar and J. J. P. C. Rodrigues, "Hybrid Deep-Learning-Based Anomaly Detection Scheme for Suspicious Flow Detection in SDN: A Social Multimedia Perspective," in IEEE Transactions on Multimedia, 2024, vol. 21, no. 3, pp.566-578

[3] Liang Xiao, Xiaoyue Wan , Xiaozhen Lu ,Yanyong Zhang , Di Wu, “IoT Security Techniques Based on Machine Learning”, IEEE 2023

[4] Marwa Mamdouh; Mohamed A. I. Elrukhsi; Ahmed Khattabi , and Qi Shi, “Securing the Internet of Things and Wireless Sensor Networks via Machine Learning:A Survey”, IEEE 2022

[5] A. Nauman, Y. A. Qadri, M. Amjad, Y. B. Zikria,M. K. Afzal and S. W. Kim, "Multimedia Internet of Things: A Comprehensive Survey," in IEEE Access, vol. 8, pp. 8202-8250, 2021.

[6] X. Wang, L. Gao, S. Mao, and S. Pandey, “CSI- based fingerprinting for indoor localization: A deep learning approach,” IEEE Trans. Vehicular Technology, IEEE 2020.

[7] J. Schmidhuber, “Deep learning in neural networks: An overview,” Neural Network, vol. 61, Jan. IEEE, 2019.

[8] Mutsam A. Jarajreh ; Elias Giacoumidis ; Ivan Aldaya ; Son Thai Le ; Athanasios Tsokanos ; Zabih Ghassemlooy ; Nick, J, “Artificial Neural Network Nonlinear Equalizer for Coherent Optical OFDM”, Volume-27, Issue-4, IEEE 2018.

[9] I Sohn, “A Low Complexity PAPR Reduction Scheme for OFDM Systems via Neural Networks”, Volume-18, Issue-2, IEEE 2017.

[10] T Ding, A Hirose, “Fading channel prediction based on combination of complex-valued neural networks and chirp Z-transform”, IEEE Transactions on Neural Networks and Learning Systems, IEEE 2017

[11] MN Seyman, N Taspinar, “Channel estimation based on neural network in space time block coded MIMO–OFDM system”, Volume-23, Issue-1, Elsevier 2016

[12] N Taspınar, M Cicek, “Neural network based receiver for multiuser detection in MC-CDMA systems”, Volume-68, Issue-2, Springer 2016

[13] T. Zhang and Q. Zhu, “Dynamic differential privacy for admm-based distributed classification learning,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 172–187, 2016.

[14] Y. Shen, C. Luo, D. Yin, H. Wen, R. Daniela, andW. Hu, “Privacy- preserving sparse representation classification in cloud-enabled mobile applications,” Computer Networks, vol. 133, pp. 59–72, 2018.

[15] M. Usman, M. A. Jan, X. He, and P. Nanda, “Data sharing in secure multimedia wireless sensor networks,” in Trustcom/BigDataSE/I SPA, 2016 IEEE. IEEE, 2016, pp. 590–597.

[16] M. Usman, N. Yang, M. A. Jan, X. He, M. Xu, and K.-M. Lam, “A joint framework for qos and qoe for video transmission over wireless multimedia sensor networks,” IEEE Transactions on Mobile Computing, vol. 17, no. 4, pp. 746–759, 2018.