A Review on Machine Learning and Deep Learning Models for Privacy Preservation in IOT and IOMT Applications

Neelima Singh[1], Prof. Pawan Panchole[2]
VITM, Indore[1,2]

Abstract: The concept of Internet of Multimedia Things (IoMT) is becoming popular now a days and can be used in various smart city applications, e.g., traffic management, healthcare, and surveillance. In the IoMT, devices, e.g., Multimedia Sensor Nodes (MSNs) are capable of generating both multimedia and non-multimedia data. The generated data are forwarded to a cloud server via 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. Thus it becomes necessary to address the aspect of data privacy while aggregation and analysis of such intermittent data from MSNs. The paper presents the previous work in the domain of privacy preserved architecture for such IoMT applications.

Keywords: Multimedia Sensor Nodes (MSNs), Internet of Things (IoT), Internet of Multimedia Things (IoMTs), Privacy Preserving Data Collection and Analysis (P2DCA).

I. INRRODUCTION

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. The definition of the Internet of things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems.[5] Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", covering devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smart phones and smart speakers. Thus IoT can be thought of a new paradigm in technology shaping future connectivity of devices. Typical applications of IoT are:

1) Smart Cities.
2) Healthcare
3) Transportation
4) Traffic Control
5) Manufacturing
6) Large Scale Automation
7) Big Data Applications etc.

Off late, IoT is also characterized by the share of multimedia data formats typically referred to as Internet of Multimedia Things (IoMT). RECENT developments in the electronic industry have enabled sensing devices to capture high-resolution multimedia data, and transformed the concept of Internet of Things (IoT) into Internet of Multimedia Things (IoMT). The most common example of these devices is Multimedia Sensor Nodes (MSNs). Prior to understanding the concepts and applications of IOMT, the conceptual model of IoT is presented in figure 1.

Figure.1 The Conceptual Model of IoT

II. PRIVACY PRESERVING DATA COLLECTION AND ANALYSIS (P2DCA) APPRAOCH

The MSNs form a network known as a Wireless Multimedia Sensor Network (WMSN). In the WMSN, captured multimedia data are forwarded to a nearby Base Station (BS) to perform computationally complex tasks and offload processed data to a cloud server. The BS is connected to the cloud server through a high-speed Internet connection. However, it is possible that the BS is unable to upload processed multimedia data to the cloud server due to technical problems in the underlying telecommunication network. In this particular situation, mobile sinks can be utilized to collect data from nominated MSNs, known as Cluster Heads (CHs), and forward to the cloud server. However, the involvement of mobile sinks for data collection in the IoMT may put the privacy of original data sources, e.g., MSNs, at risk.

The term privacy is a subjective concept and can have differ- ent illustrations. In this paper, we consider the scenario of IoMT where the end-devices are continuously capturing and uploading the multimedia data. These devices can be a part of different sensitive applications, e.g., surveillance, healthcare, and transportation management, and need to be protected from various security and privacy threats. Preserving the privacy of these devices is highly important and if it gets compromised, an intruder can use and manipulate these devices for malicious purposes. The IoMT applications, e.g., surveillance, healthcare, and transportation management, generate sensitive multimedia data that need to be uploaded on urgent bases for quick actions. To avoid the end-to-end delay, mobile sinks can be utilized to upload the collected data to cloud servers. In the mobile data collection scenario, the credibility of mobile sinks becomes a challenging task if they are anonymous. Even if the mobile sinks are registered devices, still there are chances that the privacy of IoMT devices may be compromised through malicious applications running on mobile sinks. Identities (IDs) and location information of member MSNs can easily be determined by analyzing the shared data. If the MSNs are compromised, an attacker can not only manipulate the forwarded data to generate misleading results, but also can gain access to and control the underlying network. Therefore, protecting the privacy of MSNs becomes an important and pivotal security concern in the IoMT applications.

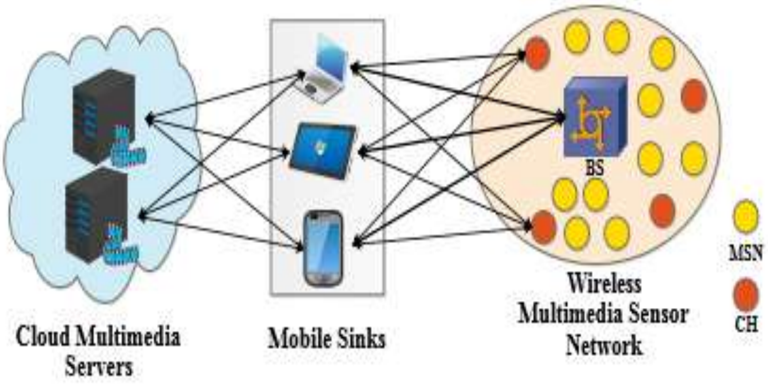

Figure.21 The IoMT Architecture

Furthermore, due to technological growth in the electronic industry, end-user devices are now powerful enough and can participate in different computing tasks, e.g., mobile computing in IoT and IoMT.

III PREVIOUS WORK

Usmaet al. in [1] proposed concept of Internet of Multimedia Things (IoMT)is becoming popular now a days and can be used in various smart city applications, e.g., traffic management, healthcare, and surveillance. In the IoMT, devices, e.g., Multimedia Sensor Nodes (MSNs) are capable of generating both multimedia and non multimedia data. This method enables the IoT gateway, which collects signals from the IoTDs, to effectively authenticate the reliability of the signals. Moreover, in massive IoT scenarios, since the gateway cannot authenticate all of the IoTDs simultaneously due to computational limitations, a game-theoretic framework is proposed to improve the gateway's decision making process by predicting vulnerable IoTDs. The mixed-strategy Nash equilibrium (MSNE) for this game is derived and the uniqueness of the expected utility at the equilibrium is proven. In the massive IoT system, due to the large set of available actions for the gateway, the MSNE is shown to be analytically challenging to derive, and, thus, a learning algorithm that converges to the MSNE is proposed.

Garg et al. in [2] proposed an approach that used the concept of deep learning for high speed optical networks in which the non-linear interference (NLI) was proposed to be mitigated by the use of a differential learning rule based on deep neural networks. The approach used the novel technique of solving the non-linear Scroodinger's equation using the negated non-linearities of the optical fibers that were laid down or used in the network. It was introduced that such an approach was called digital back-propagation. The need for deep learning as cited was the complexity of the digital data that was being transmitted in the optical fibers.

Xiao et al. in [3] proposed a technique that used the technique of deep learning for OFDM channel estimation and signal detection. It was shown that the addition of pilots would affect the BER of the system. The necessity of the deep neural networks was because of the extremely non-linear and frequency selective nature of OFDM systems wherein small or extremely narrowband spectrum is allocated to each user. Due to the channel frequency response being non-flat, several sub-carriers undergo severe fading and hence this effects the BER of the proposed system. In this approach, the BER was found to be in the order of 1/1000 and it was shown that the mean square error was relatively high for channel estimation purposes. The number of epochs to train the deep neural network (DNN) was also high i.e. 1000 iterations.

Mamdough et al. in [4] laid down machine learning platforms for next generation systems communication in networks. The focus was on 5G networks and the use of machine learning for the performance enhancement of such network using machine learning techniques. The areas of focus were the channel state information (CSI) data extraction from typical channel sounding mechanisms. The use of machine learning was also jumping from one configuration to the other estimating the BER of the system. It was shown that such systems were highly reliable and could adjust to the radio environment.

Nauman et al. in [5] proposed deep learning for the use of decoding linear codes that are used in the belief propagation approach. The performance metric used was the Bit Error Rate. The property that was leveraged in this case was the independence of the code word that is transmitted in the case of belief propagation mechanisms. The training data set is a self created bit stream of the zero codeword. The channel used is the AWGN channel. The SNR variation is done from 1 deci Bel to 6 deci Bel. The deep neural network is trained for the various block sets of BCH codes. The approach was presented as a neural or AI based approach for the design of highly accurate de-coders.

Wang et al. in [6] proposed a technique that incorporated digital fingerprinting using channel state information (CSI) and deep neural networks (DNN). The technique was termed as Deep-Fi. The areas of focus were the channel state information data extraction from typical channel sounding mechanisms. The use of machine learning was also jumping from one configuration to the other estimating the BER of the system. The proposed system was suitable for cognitive radio environments that may be existing in the proposed system's architecture.

Schmidhuber et al. in [7] put forth the basics of deep learning. It was a state of the art review on deep learning and the associated applications. It was shown that Deep neural networks generally have multiple hidden layers with or without the same number of neurons. The learning rate for each hidden layer among the multiple layers varies depending upon the design of the system but the overall gradient is decided considering the hidden layer as a whole. The performance metric is decided by the gradient and the mean square error (MSE) or root mean square error (RMSE). The variable learning rate for the different hidden layers was also proposed as a scheme to generalize and overall cost function or objective function for the deep neural network.

Jarahreh et al. in [8] proposed a technique using technique for the channel estimation of coherent optical networks using ANN. The technique was to be employed for the coherent systems in which wavelength division multiplexing (WDM) was used and it was shown that the proposed system was able to estimate the Optical Network channel. The performance of the system was computed based on the Scatter Plots and the relation was drawn with reference to the BER curves obtained. The Quality Factor (Q-Factor) was also computed. It was shown that the proposed system was able to achieve a BER of 0.001.

Sohn in [9] proposed a technique for the reduction of peak to average power ratio (PAPR) of OFDM systems based on artificial neural networks. The proposed technique uses an active constellation extension technique that is based on an ANN model at the receiving end. The system is so designed that the system attains low computational complexity. The proposed system doesn't only reduce the PAPR of the system but also reduces the BER of the system significantly. The frequency selective nature of the system introduces BER, but the ANN model at the receiving end equalizes the cannel induced errors.

Ding et al. in [10] proposed a technique that tried to compensate for the fading losses in with pre-equalization techniques and power control. This is effective to mitigate degradation of Quality of Service (QoS). The previous versions of the same design used the chirp based z- transform, the acronym for which is the CZT, used a technique of extrapolation. The concept was to find or fit missing values in the set of values available. However, an insertion of values based on average or mean, last value, or maximum occurring value can lead to erroneous results. However, the use of ANN is useful in the prediction problems wherever there is a need for estimating complex channel parameters.

IV. P2DCA BASED ON MACHINE LEARNING

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:

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

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

Both statistical estimation and machine learning consider the problem of minimizing an objective function that has the form of a sum:

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

where

W is the weight

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.

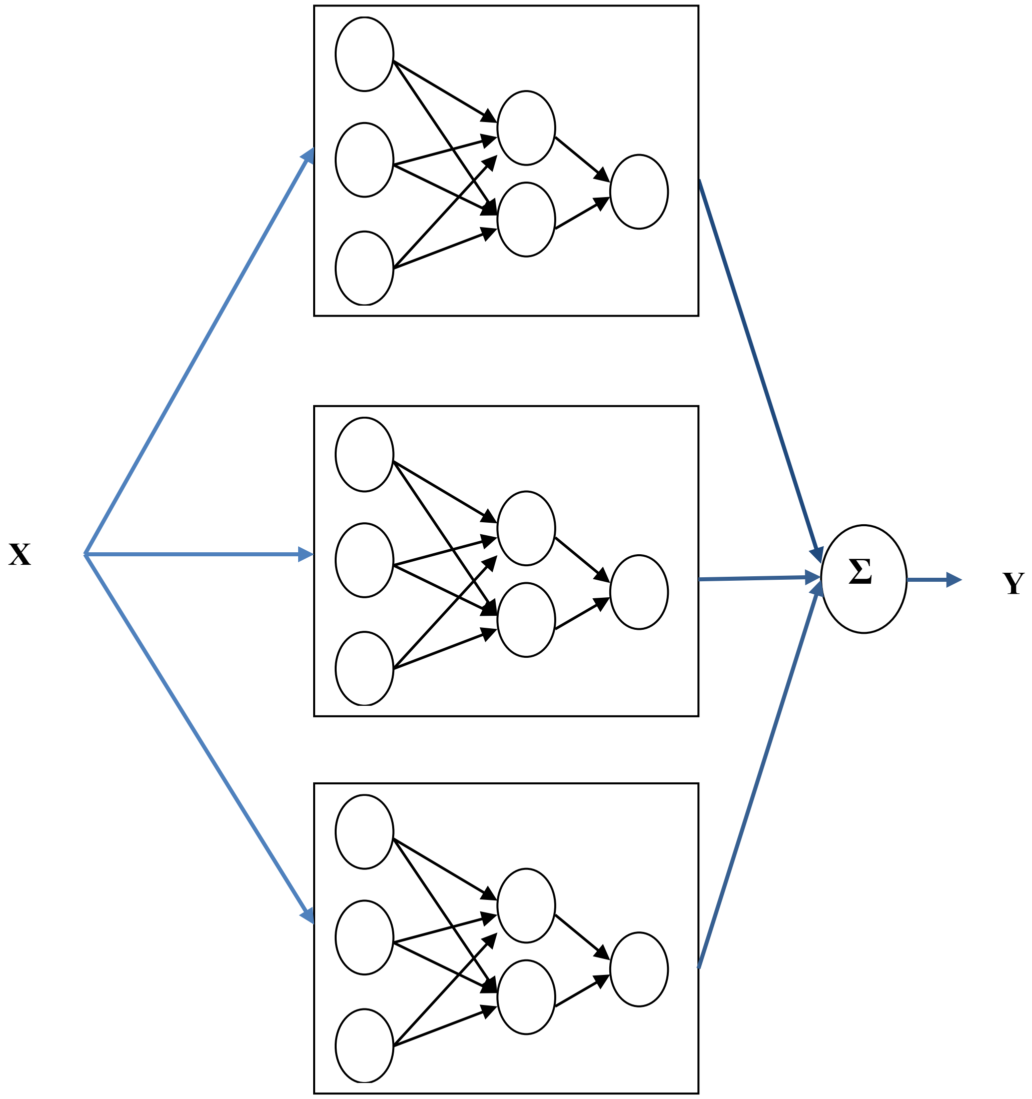

Figure.3 Bootstrapped Architecture for Neural Batch Processing

In order to build accurate neural network models, ideally a large amount of data covering different process operating conditions should be used in network training. In batch processes, data for building neural network models are usually not abundant due to limited batch runs in the manufacturing of a particular product. Thus the neural network model developed is only an approximation of the modelled batch process and model plant mismatches are unavoidable. Due to the model plant mismatches, the optimal control policy calculated on the model may not be optimal when applied to the actual process. Due to the repetitive nature of batch process operations, it would be possible to improve the operation of the next batch using the information of the current and previous batch runs. Various run-to-run control strategies for the product quality have been proposed in the literatures. The operating policy can be optimised by run-to-run optimising control for the final product quality in order to address the problems of model plant mismatches and/or unmeasured disturbances in batch processes. The performance of the system is generally computed based on the following parameters:

1) Computational Overhead
2) Data Freshness
3) Packet Delivery ratio
4) Reconstruction ratio

The overall performance metrics are mathematically defined as:

Recall: It is mathematically defined as:

$$\boldsymbol{Recall = \frac{TP}{TP+FN}} \qquad \textbf{(4)}$$

Precision: It is mathematically defined as:

$$\boldsymbol{Precisiosn = \frac{TP}{TP+FP}} \qquad \textbf{(5)}$$

F-Measure: It is mathematically defined as:

$$\boldsymbol{F - Measure = \frac{2.Precision.Recall}{Precision+Recall}} \qquad \textbf{(6)}$$

Here.
TP represents true positive
TN represents true negative
FP represents false positive
FN represents false negative

Conclusion: It this paper, the concept of internet of multimedia things (IoMT) has been illustrated with its coherence with internet of things (IoT). The privacy preserving mechanism of such networks has also been discussed. It has also been shown that one of the most effective techniques to implement the privacy preserving data collection and analysis (P2DCA) approach can be implemented using the batch processing framework for neural networks. Contemporary work in this domain has been discussed with their pros and cons. The performance evaluation parameters have also been cited.

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, and W. 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.