IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Trustworthy Privacy Preserving Framework For Machine Learning In Industrial Iot Systems

M Mounika, Vattepu Pravalika, Videm Pallavi, Shabnumyasmin

Assistant Professor, Department of CSE (DS), TKR College of Engineering and Technology, Hyderabad.
Assistant Professor, Department of CSE (AI&ML), TKR College of Engineering and Technology, Hyderabad.
Assistant Professor, Department of CSE, TKR College of Engineering and Technology, Hyderabad.
Assistant Professor, Department of CSE (DS), TKR College of Engineering and Technology, Hyderabad.

Abstract: Because Industrial Internet of Things (IIoT) devices are becoming increasingly integrated into contemporary manufacturing procedures, there has been an increase in the demand for machine learning models that are both reliable and secure inside these contexts. On the other hand, due to the sensitive nature of industrial data, a rigorous approach to the protection of their privacy is required. The purpose of this study is to offer a framework that is trustworthy and protects privacy, with the intention of facilitating machine learning applications in Industrial Internet of Things systems while simultaneously protecting sensitive information. The framework makes use of a variety of encryption methods, federated learning, and differential privacy in order to guarantee the secrecy of data, the correctness of models, and the protection of privacy. The performance of object data interchange may be improved by the utilisation of device-to-device (D2D) communication mechanisms, which can be utilised by the Internet of Things (IoT). It is the goal of Internet of Things networks to provide a vast array of services of a high quality, and a significant proportion of the devices that are responsible for providing these services are mobile. Wearables, sensors, drones, and smart cars are examples of devices that require ongoing communication despite their movement patterns. As a result, an Internet of Things design should take into consideration both Quality of Service (QoS) and mobility. By enabling devices to connect with one another directly, D2D makes it possible for them to exchange material and functionality, such as access to the Internet. In order to improve the performance of Internet of Things (IoT) communication and to provide better quality of service (QoS) for data exchange services between mobile Internet of Things devices, this article presents REMOS-IoT, which stands for a REIay and MObility Scheme. The effectiveness of the suggested architecture and algorithms was demonstrated through simulation-based testing, which demonstrated how the performance of electronic devices improved in a number of different circumstances.

Keywords: Internet of things (IoT), smart gateways, D2D, QoS, performance analysis, mobility. Industrial IoT, Machine Learning, Privacy Preservation, Decentralized Processing, Secure Communication, Data Anonymization.

I.INTRODUCTION

Through the use of Internet of Things technology in industrial settings, hitherto unattainable prospects for efficiency and optimisation have been made available. In order to fully use the potential of the enormous datasets that are produced by IIoT systems, machine learning models are an extremely important component. On the other hand, due to the intrinsically sensitive character of industrial data, it is necessary to build frameworks that protect privacy in order to guarantee the confidentiality of private information.

The incorporation of Machine Learning (ML) into Industrial Internet of Things (IIoT) systems presents a wealth of potential for improving efficiency and optimising performance. The inherently sensitive nature of industrial data, on the other hand, creates problems regarding privacy and security responsibilities. In this study, a Privacy-Preserving Framework that is specifically designed for machine learning applications inside Industrial Internet of Things environments is presented. In order to protect the privacy and confidentiality of sensitive industrial information, the framework places an emphasis on decentralised processing, secure communication, and the anonymization of data. The implementation of machine learning models in industrial settings is becoming increasingly important for data-driven decision-making as the Industrial Internet of Things (IIoT) continues to undergo development. On the other hand, protecting the confidentiality of sensitive industrial data is very necessary in order to cultivate confidence and ensure compliance with rules. The issues that are related with privacy in machine learning applications that are used inside industrial internet of things systems are addressed in this study through the proposal of a Privacy-Preserving Framework.

By 2022, it is anticipated that the Internet of Things (IoT) will have reached 18 billion gadgets that are linked to the internet [1]. Important topics of study in the Internet of Things have been identified in a recent paper published by the IEEE [2], which was based on the new paradigms brought about by the growing technology. Real-time coordination, data storage, network performance, concurrency, mobility patterns, quality of service (QoS), and other related topics are included in these categories. During the process of data transmission, innovative solutions have the potential to increase the values of some metrics, particularly those that pertain to quality of service metrics, such as latency, packet loss, and throughput. Adaptation schemes [3], scheduling strategies [5, 6], clustering algorithms and other creative communication ways [7] are some of the approaches that are utilised by solutions in order to evaluate and improve quality of service (QoS).

When they are unable to connect to any base station or when there is a limited amount of bandwidth available, Internet of Things devices are able to take use of the most recent device-to-device (D2D) communication paradigm. This paradigm enables direct mobile device intercommunication. As a result of certain devices relaying data via other devices, D2D also offers other benefits, such as the saving of energy, the enhancement of quality of service, and the optimisation of load balancing [9]. An further use of D2D has been found in cooperative vehicular networks [11]. In [12] and [14], there have been proposals for architectures that enable Internet of Things devices to employ direct-to-device (D2D) connections; however, these proposals have not specifically focused on performance.

IoT devices are connected to one another through the use of smart gateways. Device clusters are formed by smart gateways in order to increase device intercommunication, identify devices that are migrating or performing poorly, and handle admission control. ITINP is responsible for managing smart gateways and relay nodes, as well as increasing the performance of clusters. This is accomplished by computing the performance metrics of objects, rearranging items that are not performing well, and transferring them into smart gateways or relay nodes that are more appropriate.

The REMOS-IoT algorithms are designed to enhance the efficiency of communication by establishing connections between devices and the most advanced smart gateways that are currently available or to specific relay nodes. Various aspects, such as the distance between devices and smart gateways, are taken into consideration by these algorithms. Additionally, the assessment of communication performance is based on quality of service measures, which include packet loss, latency, and throughput. Additionally, they take into account the convenience of the gadget, the significance of communication, and the age of the information. Through the use of REMOS-IoT, it is anticipated that devices will demonstrate a reduction in the amount of packet loss and delay, as well as achieve a greater throughput, all while preserving the connectivity of devices that are in motion.

The authors are aware that other Internet of Things designs have also taken quality of service into consideration; but, to the best of their knowledge, these systems have not utilised factors such as object mobility, relevance, or age of information. In order to enhance the overall performance of the Internet of Things network, the REMOS-IoT architecture and solution that has been developed incorporates these measurements as well as quality of service measures and uses them in creative algorithms. The next parts will provide a detailed description of the REMOS-IoT architecture as well as the algorithms that utilise it.

II. CLUSTERING IN THE INTERNET OF THINGS

The Internet of Things makes use of clustering to improve network performance and link devices in a manner that is both more intelligent and more efficient. The year [19] saw the introduction of an Internet of Things solution for lightweight virtualization. A distributed and virtualized infrastructure was utilised for the integration of applications. Both frameworks for Internet of Things service provisioning were analysed and contrasted by the authors. One framework was based on direct contact between two collaborating devices, while the other framework involved a manager controlling the activities between cooperating devices that formed a cluster.

The implementation of a testbed was followed by testing that analysed the usage of power and resources. According to the results of the tests, lightweight virtualization makes it possible to run a broad variety of Internet of Things applications. Additionally, it enables the required degree of abstraction and offers advantages in terms of manageability and scalability. In the paper [20], the authors introduced a matching-value based Internet of Things service composition approach. The representation, discovery, detection, and composition of services were the primary focuses of the effort.

An algorithm for cluster-based distribution was also presented by the authors. This algorithm allows for a decision process that is more trustworthy and resilient. Additionally, a distributed consensus approach was presented in order to enhance the reliability and trustworthiness of the decision process using this algorithm. However, the plan did not take into account all of the stages that comprise the life cycle of services. A proposal was made in [21] for an architecture that would be used for the deployment of wireless sensor networks (WSN), which would have several sink nodes and layers. Also included in the design is a routing protocol and an algorithm for choosing cluster heads in multi-layer multi-sink clusters. The architecture takes into consideration the integration of the Internet of Things with the cloud. It is the algorithm's responsibility to do load balancing while taking into account load fairness and energy. Even if the solution does not contain peer-to-peer (P2P) connectivity, the results showed that there was an improvement in the network's lifetime.

III. MOBILITY IN THE INTERNET OF THINGS

There are a number of mobile Internet of Things devices, which presents researchers with a number of issues. In the article [22], a framework for the planning of routes during emergencies was provided. The framework takes into account mobile Internet of Things devices as well as human activity inside buildings in order to achieve the best possible evacuation timeframes. The findings indicated that the prototype operates more effectively than alternative options that are currently available. In the article [23], the authors presented a paradigm for the dynamic supply of data for smart cities. Multimedia applications for vehicle networks (VANETs) and wireless sensor networks (WSNs) are included in the framework.

With the goal of preserving high quality of service standards, the system is designed to identify optimised pathways for packets. A number of metrics, including energy, delay, and throughput, were investigated, and the findings revealed a reduction in overall latency and an extension of the network's life span. There has not yet been any research done on how the framework will behave in a more extensive network. A social Internet of Things (SIoT) architecture was proposed by the authors in [24] for the purpose of handoff between mobile and fixed access points. During group excursions, Android smartphones have the ability to facilitate the sharing, downloading, and utilisation of geo-information, which includes travel information regarding beautiful areas, landmarks, and other points of interest.

Lower levels of energy usage, service time, and cost were seen in the tests. REMOS-IoT was developed with the intention of advancing technology beyond the current state of the art, which is reflected by the methods outlined in this section. It places an emphasis on device mobility, device-to-device communications, object clustering, and quality of service awareness. REMOS-IoT makes use of cutting-edge algorithms that provide mobility support for a wide range of Internet of Things services while simultaneously preserving high levels of quality of service.

IV. REMOS-IoT ARCHITECTURE

The REMOS-IoT architecture is made up of internet of things devices that are clustered together, smart gateways, and the IoT Integration Platform (ITINP), which is a server application that is hosted in the cloud. Our prior work, which was reported in [5], is expanded upon by this architecture, which offers mobility support, direct-to-device (D2D) connections, and increased quality of service awareness through the use of the following metrics: the age of the information, location, device relevance, and performance (i.e. a score that combines loss, latency, and throughput).

In the five-layer design that was presented in [7], REMOS-IoT architectural components, such as Internet of Things devices, smart gateways, and Internet of Things Internet of Things Protocols, contribute to distinct tiers. The most important REMOS-IoT components are depicted in Figure 2, which places them within the framework of these five IoT architectural levels. The Internet of Things (IoT) items, such as smart sensors and home appliances, are stored in the items layer, which also provides support for basic D2D communication linkages between these things. Additional communication assistance between objects is made possible by the Network layer, which is comprised of smart gateways. This layer serves as a supplement to direct-to-direct interactions.

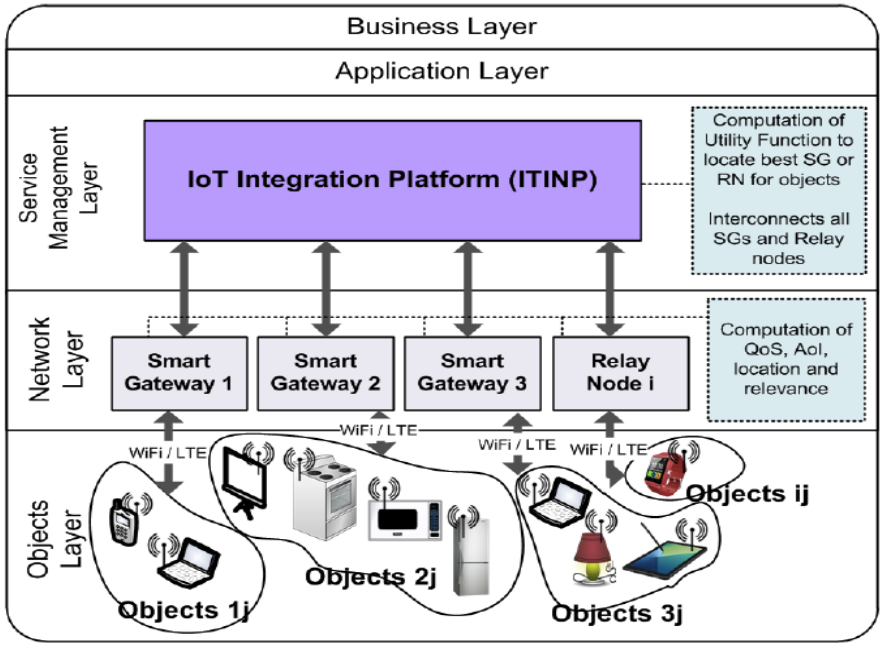

Figure 1. REMOS-IoT layered architecture.

Local Internet of Things items are clustered around the smart gateways, and they attempt to implement solutions that will increase overall communication performance by enhancing network circumstances. One of the components of the Service Management layer is the ITINP, which is responsible for collecting performance data from the smart gateways. ITINP is a component of the Service Management layer that is responsible for performing intelligent control of network connections. It also manages the interchange of different sorts of data, including sensor feedback and multimedia information, among other types of data. The apps layer is responsible for the deployment of user apps and enables individuals to communicate remotely within the framework of a variety of user services. The Business layer is home to Big Data applications, the majority of which are utilised only for the purpose of making decisions concerning policy. Components in the higher two tiers of the Internet of Things architecture are not present in REMOS-IoT.

The REMOS-IoT and its components, such as utility functions, reputation scores, and algorithms for mobility assistance and clustering, are discussed in further detail in the subsequent sub-sections. Intelligent gateways are responsible for managing admission control, calculating and storing information relating to performance, and interconnecting Internet of Things items. Additionally, they are responsible for making decisions regarding objects. The Internet of Things (IoT) items are able to interact with one another by means of the smart gateways that connect them. Due to the fact that it links all of the smart gateways that are part of the REMOS-IoT network, the

cloud-based ITINP is utilised in order to make it possible for devices to access the services that are offered by objects that are linked to other smart gateways.

Devices' mobility is supported by smart gateways since they are aware of the locations of the devices. In addition to being utilised for admission control, locations are utilised in the clustering techniques. On the basis of what can be seen in Figure 3, the object O23 is travelling in the direction of an area that is encompassed by two access points and a base station. In order to ascertain which access point or base station will respond to the connection request made by the object, gateways compute the score that determines which gateway is the most suitable to respond first when the request is made. For instance, object O21 is located closer to BS3, yet the device is more effectively linked to AP2 based on the reputation of the object and the resources that are accessible on BS3.

V.ALGORITHMIC APPROACH

Objects' reputations are evaluated by the Admission Control Unit of the Smart Gateway in order to determine whether or not to allow or reject devices. Additionally, it evaluates the performance of the gateway, which is computed by the Quality of Service Measurement Unit of Smart Gateways, in order to ascertain whether or not it is capable of supporting a new device that is being introduced. In the event that it is unable to support further devices, ITINP will choose the next smart gateway that is the most appropriate for the device. In addition, the locations of the devices are measured within this unit, and the results are subsequently communicated to the Decision Making Unit.

The Quality of Service (QoS) Measurement Unit of the Smart Gateway is responsible for retrieving the QoS metrics of devices that do not possess the resources necessary to conduct the QoS data collecting algorithm on their own. Each service is responsible for collecting these metrics. Additionally, it is the responsibility of this unit to gather quality of service measurements from the smart gateways. This allows for the performance of the gateway to be evaluated for the purpose of controlling the admittance of incoming devices. Moreover, this unit is responsible for calculating the age of the information in connection to the communications that take place between the gateway and the devices.

Algorithm 1 Providing Mobility Support for Objects

```
if (L_ij <= threshold) then
    SG_i broadcasts message with O_ij and L_ij
    SG_i waits other SGs and RNs (within O_ij range) reply
    O_ij receives message broadcasted by SG_i
    O_ij broadcasts message to SGs and RNs
    SGs and RNs compute L_ij received from O_ij
    SGs and RNs send message with L_ij and U_ij to SG_i
    SG_i selects best L_ij + U_ij
    if (SG_i has best L_ij + U_ij) then
        return
    end
    else
        SG_i notifies SG/RN with best L_ij + U_ij
        SG/RN.attach(O_ij)
        SG_i.detach(O_ij)
    end
end
```

It is the responsibility of the Decision Making Unit of the Smart Gateway to compute metrics and rank devices in respect to relevance, quality of service, location, and age of information scores.
In addition to this, it identifies items that are migrating or have poor performance and may eventually be reassigned to other gateways or relay nodes. In section III.C, the QoS Calculator unit is responsible for evaluating the functions that are described in equations (1) and (2). On the other hand, the Relevance Calculator is responsible

for computing the number of packets that are transferred between devices and gateways in order to determine which clusters are closely associated to a particular device.

11 devices in WiFi + 11 devices in LTE					
No. Devs.	Device Type	Scenario1 (Mbps)	Scenario2 (Mbps)	Scenario3 (Mbps)	Traffic Direction
1	High Bitrate	10	20	30	DL only
1	Avg. Bitrate	5	10	15	DL only
1	Low Bitrate	2	4	6	DL only
7	Very Low	0.4	0.8	1.2	UL & DL
1	Mobile Device	1	2	3	UL & DL
Total Bitrate		20.8	41.6	62.4	
22 devices in WiFi + 22 devices in LTE					
No. Devs.	Device Type	Scenario4 (Mbps)	Scenario5 (Mbps)	Scenario6 (Mbps)	Traffic Direction
2	High Bitrate	5	10	15	DL only
2	Avg. Bitrate	2.5	5	7.5	DL only
2	Low Bitrate	1	2	3	DL only
14	Very Low	0.2	0.4	0.6	UL & DL
2	Mobile Device	0.5	1	1.5	UL & DL
Total Bitrate		20.8	41.6	62.4	
100 devices in WiFi + 100 devices in LTE					
No. Devs.	Device Type	Scenario7 (Mbps)	Scenario8 (Mbps)	Scenario9 (Mbps)	Traffic Direction
95	Very Low	0.208	0.416	0.624	UL & DL
5	Mobile Device	0.208	0.416	0.624	UL & DL
Total Bitrate		20.8	41.6	62.4	

Table 1. REMOS-IoT scenarios description.

As metrics for device location, REMOS-IoT makes use of the RSSI that is gathered by gateways in Wi-Fi access points (AP) and the RSRP that is gathered by gateways in LTE base stations (BS). RSSI is provided by even the most basic Internet of Things devices, such as beacons, which is why these metrics were selected. It is possible to estimate distance using RSSI-based approaches, which are advantageous because to their low cost, low power consumption, and accessibility. They are now utilised in a variety of systems.

When devices display low dBm, which indicates that they are likely moving away from the gateway, REMOS-IoT makes judgements. This is because -90 decibel-milliwatts (dBm) is considered to be a low RSSI. The overall utility function that was utilised in the process of calculating the reputation score. REMOS-IoT computes the reputation of a device in respect to the smart gateways in order to find a balance between performance, age of information, relevance and location of devices, resulting in a normalised Uij reputation score per object.

$$U_{ij} = wp\frac{P_{ij}}{\max\limits_{j}(P_{ij})} + wr\frac{R_{ij}}{\max\limits_{j}(R_{ij})} + wa\frac{A_{ij}}{\max\limits_{j}(A_{ij})} + wl\frac{|L_{ij}|}{\max\limits_{j}(|L_{ij}|)}$$

VI. PERFORMANCE ANALYSIS

In order to conduct tests, the REMOS-IoT was simulated and analysed with the help of the NS-3 simulator [3], as shown in Figure 2. In Table 1, the parameters that were used in the simulation setup, such as the simulation time, mobility speed, data rates, and models of both the antenna and the mobility, as well as their respective measurements, are shown. In the REMOS-IoT algorithms, the reputation score (Uij) was given equal weights, which means that the weights were written as follows: wp = wr = wa = wl.

Parameter	Value
Simulator	NS-3.24.1
Duration of the Simulation	14s+10s before and after sim.
Initial dist. between nodes and antennas	3 metres
WiFi and LTE Data Rates	40 Mbps and 100 Mbps
WiFi Standard	802.11ac (40MHz, MCS 9)
LTE eNB Antenna Model Type	Isotropic Antenna Model
Remote Station Manager	ConstantRateWifiManager
Mobility Model	ConstantVelocityMobilityModel
Speed of Smart Watch user	2 metres per second

Table 2. Simulation setup.

Nine different scenarios were constructed using clusters that represented smart homes and companies that contained Internet of Things equipment. These scenarios are displayed in Table 2. Smart watches are an example of mobile devices that are situated in a smart home together with other Internet of Things gadgets. These devices are all connected to one another through a local gateway that utilises a WiFi 802.11ac access point. These mobile devices travel towards another smart home, and when they are no longer within the range of both gateways, they must establish a connection with a relay node using direct-to-device (D2D) communications in order to reconnect to the internet.

With downlink only, each gateway of the two smart homes, one of which is connected to WiFi access points and the other to an LTE base station, supports a number of different types of devices in WiFi and LTE networks. These include three smart objects with high, average, and low bitrates (for example, in scenario 2, these device types have 20, 10, and 4 Mbps, respectively, representing video devices); and seven smart objects with very low rates, which simulate a variety of mobile and non-mobile Internet of Things objects. Within the scenarios, the mobile devices transition from the WiFi local area network (LAN) to the LTE network.

When the device is in between networks or outside of their coverage area, a relay node that is accessible will offer a direct-to-device shared connection. This ensures that the smart watch continues to operate inside the ITINP platform.

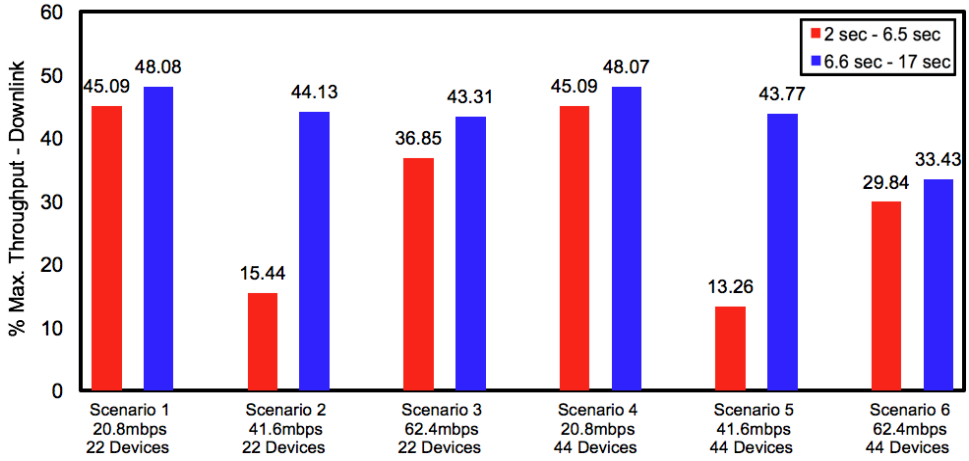

Figure 2. WiFi - Downlink - % Max. Thru. of devices with high consumption.

In addition to the several types of devices that were evaluated in each scenario, a variable number of devices were examined: 22 devices were examined in situations 1, 2, and 3, 44 devices were examined in scenarios 4, 5, and 6, and in scenarios 7, 8, and 9, 200 devices were examined. It was determined that the WiFi network was home to half of the devices, while the LTE network was home to the other half. Initially, the mobile devices are connected to the WiFi network, and then they progress to the LTE network. Only device types with a very low bitrate were included in the scenarios with 200 devices (i.e. devices 7, 8, and 9). These scenarios reflect an Internet of Things network that has a large number of limited devices.

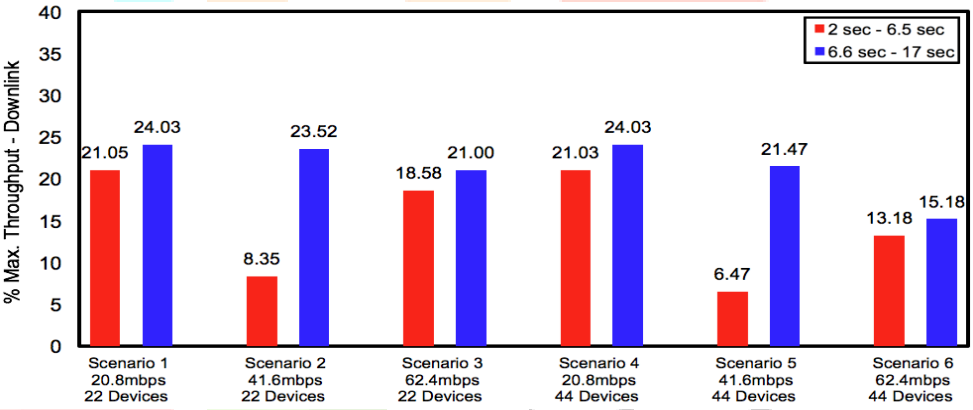

Figure 3. WiFi - Downlink - % Max. Thru. of devices with avg. consumption.

It is possible to switch from one network to another without any interruptions when mobile devices are connected to the internet continuously. Throughputs that are high are being obtained in the majority of circumstances, both in the uplink and the downlink. Scenario 9, which had a large number of devices and high bitrate needs (i.e., 200 devices and a total bitrate of 62.4 Mbps), had fewer benefits in regard to throughput than previous situations because of the amount of congestion that this scenario experienced. Despite this, mobile devices, for example, had an increase of 83% in the throughput that they were able to accomplish in this scenario.

The delays that occurred in WiFi and LTE scenarios, both in the uplink and downlink directions, were significantly reduced. An example of this would be scenario 6, in which a high delay of 265.1 milliseconds was reduced to 5 milliseconds for moving devices. When it came to downlink, the average latency for devices that were connected to WiFi, LTE, and mobile networks was reduced by 43 percent, 17 percent, and 92 percent, respectively, across all situations. There was a 27% drop in latency for WiFi, 26% decrease for LTE, and 23% decrease for mobile devices when it came to uplink.

	Delay (ms)		Loss (%)	
	IoT - RTP & IoT - RTCP	REMOS-IOT	IoT - RTP & IoT - RTCP	REMOS-IOT
Average	204.74	7.53	2.50	0.43
St. Dev.	2.83	0.11	1.34	0.08
Max. Value	211.00	7.75	5.00	0.60
Min. Value	200.00	7.25	1.00	0.35
T-test p-value	6.9×10^{-35} (<0.05)		3.25×10^{-6} (<0.05)	

Table 3. Comparison of the works.

Overall, there was a significant decrease in the amount of packets that were lost. When all possible circumstances were taken into consideration, the average amount of packet loss in the downlink was reduced by 51%, 36%, and 92% for mobile devices, WiFi, and LTE, respectively. The amount of loss experienced by WiFi, LTE, and mobile devices was reduced by 44%, 51%, and 80% respectively in proportion to the uplink.

The Internet of Things Real-Time Protocol (IoT-RTP) and Internet of Things Real-Time Communication Protocol (IoT-RTCP) protocols, which are implemented on the Network Simulator 2 (NS-2), utilise a revolutionary method that divides huge multimedia sessions into simpler sessions while maintaining knowledge of the condition of the network. Despite the fact that REMOS-IoT was implemented on NS-3, there were no significant changes discovered when comparing the schemes in regard to the simulator that was utilised, and the findings were identical. Delays and packet losses were averaged over time in all of the devices that were part of the second WLAN after REMOS-IoT algorithms were implemented. This was done for the purpose of establishing a baseline comparison. An analogous simulation runtime was taken into consideration.
It is possible to view the findings that were acquired in Table 3. When taking into consideration the average load scenario 2 of REMOS-IoT, it is clear that REMOS-IoT performs better than the other schemes, with a latency that is 96.3% lower and a packet loss that is 82.6% lower. Following a study of the results of a paired student t-test, the low p-value of 6.9 x 10-35 for delay and 3.25 x 10-6 for packet loss demonstrates that REMOS-IoT is statistically significant in favour of both delay and loss samples. This is proven by the fact that the p-value values were achieved.

VII. CONCLUSION

The purpose of this study is to propose a framework for machine learning in industrial Internet of Things systems that is reliable and protects users' privacy. The framework tackles the issues that are connected with maintaining data confidentiality in contexts that are associated with the Internet of Things (IoT) by integrating sophisticated encryption methods, federated learning, and differential privacy. The technique that has been described makes it possible to deploy machine learning models in industrial settings while protecting sensitive information. This helps to create a secure and efficient integration of technologies related to the Industrial Internet of Things (IIoT).
The purpose of this work was to present REMOS-IoT, which was designed to increase the performance of mobile Internet of Things device communication by enhancing the existing Internet of Things architecture using algorithms. For the purpose of efficiently clustering Internet of Things devices and improving their communication performance while simultaneously enabling device mobility, REMOSIoT keeps score records for quality of service (QoS), relevancy, age of information, and location. A WiFi-only smart watch is set up in a smart home together with a number of other smart devices that are first linked to a local gateway through the use of a WiFi 802.11ac access point. This is the scenario that will be tested. In order to keep the quality of service at a high level, the smart watch experiences a loss of connection and must make use of the REMOS-IoT algorithms that have been suggested. All of the findings for uplink and downlink were documented in terms of throughput, packet loss, and latency. The solution was evaluated through the use of NS-3 modelling and simulations. When compared to competing solutions, REMOS-IoT performs better in terms of these quality of service parameters. A Privacy-Preserving Framework is presented in this study. Its purpose is to solve the specific issues that machine learning applications in industrial Internet of Things systems provide. A solid solution for protecting sensitive industrial information is provided by the framework, which places an emphasis on decentralised processing, secure

communication, and the anonymization of data. The technique that has been described makes it easier to deploy machine learning models in industrial settings in a responsible and safe manner, which in turn encourages the wider adoption of data-driven decision-making among businesses.

REFERENCES

[1] Ericsson. (2020). Internet of Things forecast Ericsson Mobility Report.

[2] N. Narendra and P. Misra. (2016). Research Challenges in the Internet of Mobile Things.

[3] G.-M. Muntean, P. Perry, and L. Murphy, ``Objective and subjective evaluation of QOAS video streaming over broadband networks," IEEE Trans. Netw. Service Manage., vol. 2, no. 1, pp. 19-28, Nov. 2005.

[4] C. H. Muntean and J. McManis, ``End-user quality of experience oriented adaptive E-learning system," J. Digit. Inf., Special Issue Adapt. Hypermedia, vol. 7, no. 1, pp. 1-13, 2006.

[5] Ravindra Changala, Framework for Virtualized Network Functions (VNFs) in Cloud of Things Based on Network Traffic Services, International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume 11, Issue 11s, August 2023.

[6] S. Ezdiani, I. S. Acharyya, S. Sivakumar, and A. Al-Anbuky, ``Wireless sensor network softwarization: Towards WSN adaptive QoS," IEEE Inter-net Things J., vol. 4, no. 5, pp. 1517-1527, Oct. 2017.

[7] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, ``Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges," IEEE Wireless Commun., vol. 24, no. 3, pp. 10-16, Jun. 2017.

[8] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, ``Internet-of-Things-based smart environments: State of the art, taxonomy, and open research challenges," IEEE Wireless Commun., vol. 23, no. 5, pp. 10-16,Oct. 2016.

[9] Ravindra Changala, Block Chain and Machine Learning Models to Evaluate Faults in the Smart Manufacturing System, International Journal of Scientific Research in Science and Technology, Volume 10, Issue 5, ISSN: 2395-6011, Page Number 247-255, September-October-2023.

[10] Ravindra Changala, AIML and Remote Sensing System Developing the Marketing Strategy of Organic Food by Choosing Healthy Food, International Journal of Scientific Research in Engineering and Management (IJSREM), Volume 07 Issue 09, ISSN: 2582-3930, September 2023.

[11] Z. Zhou, H. Yu, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, ``Dependable content distribution in D2D-based cooperative vehicular networks: A big data-integrated coalition game approach," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 3, pp. 953-964, Mar. 2018.

[12] H. Rahimi, A. Zibaeenejad, and A. A. Safavi, ``A novel IoT architecture based on 5G-IoT and next generation technologies," in Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON), Nov. 2018, pp. 81-88.

[13] Ravindra Changala, A Novel Approach for Network Traffic and Attacks Analysis Using Big Data in Cloud Environment, International Journal of Innovative Research in Computer and Communication Engineering: 2320-9798, Volume 10, Issue 11, November 2022.

[13] Z. Zhou, M. Dong, K. Ota, G. Wang, and L. T. Yang, ``Energy efficient resource allocation for D2D communications underlaying cloud-RAN-based LTEF A networks," IEEE Internet Things J., vol. 3, no. 3,pp. 428-438, Jun. 2016.

[14] X. Liu and N. Ansari, ``Green relay assisted D2D communications with dual batteries in heterogeneous cellular networks for IoT," IEEE Internet Things J., vol. 4, no. 5, pp. 17071715, Oct. 2017.

[15] T. Petric, M. Goessens, L. Nuaymi, L. Toutain, and A. Pelov, ``Measurements, performance and analysis of LoRa FABIAN, a realworld implementation of LPWAN," in Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC), Sep. 2016, pp. 1-7.

[16] R. Hassan, A. M. Jubair, K. Azmi, and A. Bakar, ``Adaptive congestion control mechanism in CoAP application protocol for Internet of Things (IoT)," in Proc. Int. Conf. Signal Process. Commun. (ICSC), Dec. 2016, pp. 121-125.

[17] Ravindra Changala, “Diminution of Deployment Issues in Secure Multicast System with Group Key Management” published in International Journal of Computer Application (IJCA), Impact Factor 2.52, ISSN No: 2250-1797, Volume 2, Issue 3, June 2012

[18] I. Awan, M. Younas, and W. Naveed, ``Modelling QoS in IoT applications," in Proc. 17th Int. Conf. Netw.-Based Inf. Syst., Sep. 2014, pp. 99-105.

[19] R. Morabito, I. Farris, A. Iera, and T. Taleb, ``Evaluating performance of containerized IoT services for clustered devices at the network edge," IEEE Internet Things J., vol. 4, no. 4, pp. 1019-1030, Aug. 2017.

[20] S. Li, G. Oikonomou, T. Tryfonas, T. M. Chen, and L. Da Xu, ``A distributed consensus algorithm for decision making in service-oriented Internet of Things," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1461-1468, May 2014.

[21] W. Twayej, M. Khan, and H. S. Al-Raweshidy, ``Network performance evaluation of M2M with self organizing cluster head to sink mapping," IEEE Sensors J., vol. 17, no. 15, pp. 4962-4974, Aug. 2017.

[22] L.-W. Chen and J.-J. Chung, ``Mobility-aware and congestion-relieved dedicated path planning for group-based emergency guiding based on Internet of Things technologies," IEEE Trans. Intell. Transp. Syst., vol. 18, no. 9, pp. 2453-2466, Sep. 2017.

[23] L. Li, S. Li, and S. Zhao, ``QoS-aware scheduling of services-oriented Internet of Things," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1497-1507, May 2014.

[24] Y. Li, K. Chi, H. Chen, Z. Wang, and Y. Zhu, ``Narrowband Internet of Things systems with opportunistic D2D communication," IEEE Internet Things J., vol. 5, no. 3, pp. 1474-1484, Jun. 2018.

[25] Z. Zhou, K. Ota, M. Dong, and C. Xu, ``Energy-efficient matching for resource allocation in D2D enabled cellular networks," IEEE Trans. Veh. Technol., vol. 66, no. 6, pp. 52565268, Jun. 2017.

[26] M. L. M. Peixoto, D. L. Filho, C. Henrique, D. Segura, B. Tardiole, and B. Guazzelli, ``Predictive dynamic algorithm: An approach toward QoS-aware service for IoT-cloud environment," in Proc. IEEE Int. Conf. Comput. Inf. Technol. (CIT), Dec. 2016, pp. 686-693.