2022 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE) | 978-1-6654-7280-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/WISEE49342.2022.9926943

SDN-based Federated Learning approach for Satellite-IoT Framework to Enhance Data Security and Privacy in Space Communication

Ryhan Uddin
Dept of EECS
Cleveland State University
Cleveland, OH, USA
r.uddin73@vikes.csuohio.edu

Sathish Kumar
Dept of EECS
Cleveland State University
Cleveland, OH, USA
s.kumar13@csuohio.edu

***Abstract*— The proliferation of IoT devices and integration of machine learning technologies paved the path towards automation in various sectors guided by Artificial intelligence (AI). It enables multitudes of use cases ranging from mass scale cloud-edge computing based robust communication between smart IoT devices, weather variation detecting low powered remote sensor nodes residing on a harsh terrain, AI- assisted driverless vehicles immaculately cruising through traffic to industrial robots performing sophisticated tasks with precision and finesse. As space colonization is a becoming a myth of the past and venturing towards reality, this AI-based IoT ubiquity will also be a major mart of those space colonies where autonomous infrastructures with be the norm. These IoT integrated networks will also boast a wide area of coverage reaching the furthest of the horizons with low orbit satellite integration. However, the mass deployment of these modern technologies is heavily contingent to the fact that data is safeguarded from malicious intrusions. Therefore, in this paper we have proposed an approach to thwart data breach that can plague satellite-IoT framework with respect to space communication. The framework is based on software defined networking that uses federated learning techniques for distributed systems and employs deferential privacy while sharing data among devices to ensure secured critical data transmission between IoT devices.**

Keywords—Data Privacy, Software defined network (SDN), Federated Learning, Satellite and Internet of things (IoT).

I. INTRODUCTION

Humans have always been fascinated with deep space exploration and colonization in another planet. As our planet Earth is threatened towards instability due to excessive extraction of natural resources and massive surge in carbon footprints caused by aggressive industrialization, this urge to colonize an alien terrain is only inevitable. To satisfy this inevitability, numerous projects are now undergoing from government-funded projects to private aerospace companies. NASA, being one of the long-standing frontrunners who helmed several space glories, has taken a huge step with the successful touchdown of Mars with Perseverance rover in the first quarter of 2021 [1]. Having a similar aim, Elon Mask's Space Exploration Technologies Corp. (SpaceX) is also taking massive initiatives with the ultimate goal to colonize mars by sending 1 million people by 2050 and starting with the first human touchdown of Mars by year 2029 [2].

As this colonization endeavors slowly coming into fruition, so is the necessity of integration of advanced and evolving technologies. IoT will be a massive part of this extra-terrestrial expansion as it reaches about 14.4 billion terrestrial connections as per 2022. Being one of the key communication strategies, that uses 5G/6G mobile networking technologies, systems will be deployed with the coverage over space, air, ground interconnected network (SAGIN) will heavily incorporate IoT devices [3]. Numerous essential services such as smart transportation [4, 5], smart agricultural system [6], smart healthcare [7, 8], A.I. assisted driving [9], intelligent disaster management system [10, 11, 12], unmanned aerial vehicles (UAV) [13, 14], environment monitoring system [15, 16] etc. heavily forecast the ubiquity of IoT in space colonization. Following fig. 1 gives an overview of IoT expansion in space colonization.

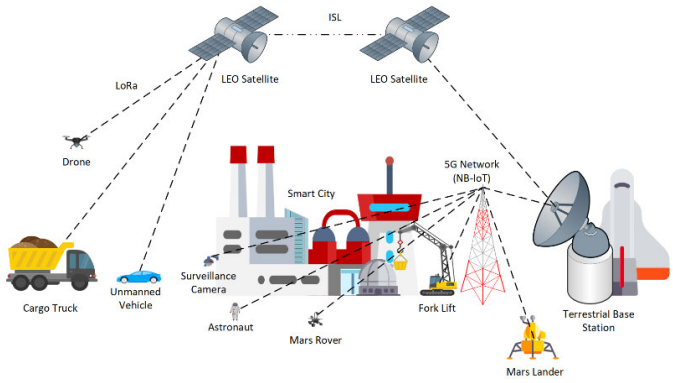

Fig. 1. Satellite-IoT setup for space colonies

Therefore, a network system comprising of satellite-IoT integration is the optimal choice for space colony communication as there are places where an optical based networks or a base station based cellular network might not be a possibility. Being an alien terrain, there might be multitudes of variables that can act as roadblocks to install a ground based cellular base stations, as there might be remote zones with harsh environments and uneven terrains, inaccessible or hazardous zones with limited accessibility. Therefore, an orbital satellite can be more effective in case for coverage, mobility and reliability. Hence a satellite-IoT approach is the most suitable to

ensure network coverage both in earth (remote areas) and also in an extra-terrestrial planet.

However, with the IoT pervasiveness comes critical security vulnerabilities. Due to the ease of access of IoT devices, they fall prey to malicious cyberattacks and causes data breach. According to a report conducted by Zscaler [17], since the year of 2019 attacks on IoT devices have increased to an astounding number of 700% [18]. According to another report, about 82% of the healthcare organizations has been a victim of IoT based cyber-attacks threatening users data privacy. This number is growing everyday as more and more devices are being added into the internet hyperspace. Therefore, it is imperative to construct a strong security backbone for IoT heavy networks.

Therefore, through this work we have explored a network framework that uses SDN as a backbone and uses satellite and IoT incorporation with the federated learning (FL) approach. The Satellite-IoT assimilation ensures network connectivity even in remote unreachable places and the SDN-based FL approach ensures the data security and privacy in propagation.

Rest of the manuscript is organized as follows. Section 2 explains about the related works in the literature. Section 3 explains the background of the tools associated with the proposed approach. Section 4 explains about the proposed approach and framework. Finally section 5 concludes with the concluding remarks and future work recommendations.

II. Related works

There are few existing works to implement Satellite-IoT based network architectures. In [19] Sanctis et al., provided an integrated satellite-IoT based communication that explores applicability of specialized MAC protocols for sensor networks and satellite resources. They have also worked on heterogeneous network interoperability, quality of service (QoS) and efficient IPv6 satellite support with group based communications. In this work, Sanctis et al., gave paramount importance to internet of remote things (IoRT) and proposed satellite communication that can directly operate in tandem with M2M (machine-to-machine) applications and remote controller actuators in smart grid scenarios [19]. Their work portrays a comprehensive scenario where these technologies can be leveraged to efficiently manage power production, seamless transmission and proper distribution. Nevertheless, this theoretical concept shows much promise but more empirical data is necessary that takes account of real life communication infrastructures with accurate results. Nonetheless, the theorized system has solid implications where nano satellites might be the only viable option as LEO satellite might be an expensive venture. Lastly, their work does not really focus on mass data centric networks with an urban setup or space colony network infrastructures based on software defined networks which is one our core concept as it provides more control over the network.

In [20] Chen et al., first evaluated the best candidate for 6G AI-based wireless communications, the LEO satellite based Satcom and explored possible machine learning techniques that can be combined with satellite networks. They have proposed federated learning based approach with four different setup for the satellite-IoT network architecture. The modes are remote cloud learning (centralized model), on board satellite learning (centralized model) and federated learning where in one of the satellite works just as relay and the other satellite acts as the server itself. The experiment was simulated using PyTorch platform with convolutional neural network (CNN) for the local user modeling. For federated learning, FedAvg [21] was used to aggregate the local models into global models. All of the setups were tested using MNIST dataset and were tested based on evaluation metrics such as communication load, training loss and accuracy. The tests show a federated learning based model is more potent but the underlying deployment cost questions the viability of the system. Nevertheless, authors have suggested an SDN/NFV based approach for the maximum utilization of the scarce satellite resources, which is one of the core element of our satellite-IoT network as SDN offers robustness in customized network orchestration.

Flauzac et al., [22] used SDN platform and incorporated wired, wireless, ad-hoc, IoT and sensor networks pertaining to a distributed network architecture. Their work is partly similar to our proposed framework which partially mirrors the terrestrial backhaul of our framework comprised of SDN controlled IoT network but excluding the satellite backhaul. However, they have identified the limitation of singular point of vulnerability and therefore, incorporated two controllers into their proposed framework referring to open controllers like OpenDaylight in order to counter data intrusions and adding fault tolerance to the network. They have used Open vSwitch for their platform which uses OpenFlow as the default standard for SDN. The network is segmented into separate extended domains that are operated with border controllers that are interconnected with each other. Each border controller is responsible for safeguarding its own domain operating in a grid security fashion. The Overall system is a promising terrestrial network architecture but pose a major drawback of having too much overhead, which can not be evaluated as the system is a prototype and has not been tested for real life network setup.

To address the existing limitations, in our proposed system, we have combined the aforementioned core SDN structure while maintaining a distributed IoT network infrastructure for the terrestrial backhaul. Having centralized controllers help to employ policies with ease and having a secondary controller with load balancer helps to avoid possible cascading failures [23]. Moreover, utilization of a dedicated decoy setup on top of extensive security policies makes security threats nearly obsolete. Additionally, the federated learning approach ensure preservation of critical data privacy and secured AI modeling through localized model training on each IoT devices. In later segments of the paper, we have discussed the tools that are needed for our framework (section III) and the implementation of the framework (section IV).

III. Tools for our framwork

A. Satellite communication

We are at an age where satellite communication is pivotal for planet wide expansion of data connectivity. In spite of our rich history, we are yet to cover a vast portion of this giant globe due to constraining factors of either economic viability or terrestrial reachability. However, these limitations can be overcome with usage of orbital satellites. There are several

kinds of satellites such as geostationary (GEO satellites), medium Earth orbit (MEO satellites), and low Earth orbit (LEO satellites) etc. The GEO satellites usually reside about 35,800 kilometers (22,300 miles) [34] above earth and usually synchronizes its position with the rotation of earth essentially keeping it stationary relative to earth's position (covering same points on the ground). As a result, it takes similar time to complete one orbit that is 24 hours. One GEO satellite can cover about one third of the earth therefore, three satellites can cover the whole planet. Traditionally these satellites are used for TV and radio broadcasting and weather data collections etc. However, due to latency it is not a viable option for instant data communications such as voice data, video calling or lag free gaming etc. In the medium Earth orbit, about 5,000 to 12,000 km (3,100 to 7,500 miles) above the earth orbits MEO satellites. Since they maintain a lower altitude from earth comparing to the GEO satellites, they offer lower latency. Therefore, MEO satellites are excellent medium for fast broadband communication. About 24 MEO satellites can cover the whole planet and the most well known usage of this satellite is the GPS (Global positioning system) and other GPS like systems such as Galileo (Europe), GLONASS (Russia), and BeiDou (China) [35]. Nevertheless, the whole process of launching GEO and MEO satellites to that high altitude above earth is economically draining. Therefore, the best solution for an IoT based communication backbone are the LEO satellites that are not only economically viable but also offers lower latency over the other alternatives [36]. A LEO satellite can orbit the earth in 1.5 hours only. However, due to a lower altitude from earth, which can range between 160 km to 2000 km, more LEO satellites are needed for wider terrestrial coverage. Hence, multiple LEO satellite work together to constitute LEO constellations. As LEO satellites are constantly in motion over earth's orbit, one single satellite might not offer consistent coverage, therefore these LEO constellations work in tandem to offer the best possible connectivity. The following figure (fig. 2) gives an overview of the three satellite categories.

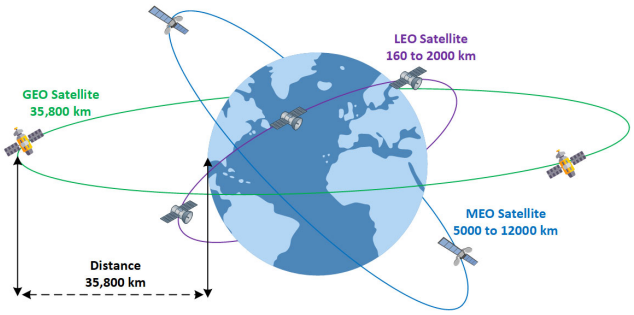

Fig. 2. Different orbital Satellites (GEO, MEO and LEO)

One of the big names in LEO constellations communication service is Iridium [37]. Iridium has a massive network coverage with over 65 satellites orbiting the earth at a speed of 17,000 mph. With the goal of uninterrupted network coverage, their satellites even have converge over the north pole of earth where most commercial satellites do not offer service. Iridium uses L band frequency, which operates in low frequencies ranging from 1,530 MHz to 2.7 GHz [38] with a longer wavelength. Therefore, it is resilient in terms of adverse weather conditions having much lower rain fade, which is common phenomena for larger parabolic antenna systems typically used by other bands like Ku and Ka [39]. Hence, planetary Mesh of LEO satellites with similar band setups are excellent tool for extra-terrestrial communication network expansion especially on harsh and inaccessible terrains with adverse weather conditions.

B. IoT

For long range IoT expansion in accessible parts of the planet, we aim to incorporate the low power wide area network (LPWAN) that operates on Narrowband IoT (NB-IoT). It is adopted by the 5G technologies due its substantial usage in massive Machine Type Communication (mMTC) [40]. Moreover, it shares many attributes of 5G NR (new radio), which is new generation radio access technology (RAT) developed by 3GPP (3rd Generation Partnership Project). Both has sub-carrier frequency of 15kHz and similar time domain structures, therefore these compatibilities of physical layer numerologies make them ideal co-operators. Nevertheless, NB-IoT by design is suitable for low powered IoT devices that have long battery life, high system capacity, very low cost and wide area of coverage therefore making it perfect for extra-terrestrial satellite-IoT network expansions [41].

Moreover, there are other forms of 5G technologies as per use cases that can be applied on high demand zones such as inhabitant colonies. For example, the Ultra-Reliable Low Latency Communication (URLLC) and also the enhanced form namely Enhanced Ultra-Reliable Low Latency Communication (eURLLC) are best suited for ultra-reliable connectivity with very little propagation latency of as low as 1 millisecond (ms). This kind of wireless technology is best suited for emergency response services, autonomous vehicles, industrial robots, critical valves and drones etc. Also there is enhanced Mobile Broadband (eMBB) or predominantly known as high speed 5G leverages the larger bandwidth spectrum of 5G providing seamless user experience with augmented and virtual reality (VR) applications, industrial routings etc. However, for the sake of simplicity, we have only incorporated NB-IoT for the satellite-IoT framework. But, those technologies can also be incorporated in the framework as per user requirements based on specific use cases.

In terms of remote inaccessible zones or furthest harsh terrains, we recommend LoRa (Long Range). It is a long range radio propagation technology that leverages a spread spectrum modulation technique derived from chirp spread spectrum (CSS) [43]. It allows mitigation of signal interference and multipath fading but it does not provide a superior communication like the NB-IoT. However, LoRa is capable of covering a vast area that can range from 15 km to 250 km depending on the line of sight, which is perfect for communication with LEO satellites. For practical example, in Belgium, the entire country's LoRa network is covered by only 7 base stations, which roughly equates to 30,500 km^2 of land

area [44]. In addition, LoRa is perfect for devices that require very little power and need to transmit signal over very long distances, in our case, a direct communication with LEO satellites. LoRa can be used for very small sensors nodes, UAV, drones, maritime equipment, space transportation, weather or temperature monitoring sensors etc. that are heavily reliant on incumbent characteristics like energy efficiency, low power consumption and very long range uninterrupted signal propagation.

C. *Satellite-IoT integration*

Now that we have set the propagation standards, the LEO satellites can easily communicate with individual network elements based on their terrestrial positions. All the LEO satellites in the LEO constellation are connected through inter satellite links (ISL) making up the whole satellite backhaul. Satellite to ground communication can happen in two ways.

The LoRa enabled low power sensors directly communicate with the satellite and then satellite relays this data to the nearest base station for further data processing. This communication can also be done through a LoRa gateway that has interconnected low powered internet of things in the vicinity. This LoRa gateway synchronizes with all of these IoTs and directly connects to the satellite for data transmission and it is followed up by the base station communication.

The other mode is the interconnectivity (using traditional satellite communication protocols) with a terrestrial satellite gateway that forwards the data to the respective cellular base stations. These base stations supports 5G technology like NB-IoT, URLLC, eMBB, nMTC etc. Each of these base stations are controlled by SDN controllers that control all network elements in that particular network. The SDN controller utilizes network slicing to segment user network into different network slices and employ different 5G protocols and access policies based on user requirements and device types. That is how space colonies or populated zones connect their terrestrial backhaul with satellite backhaul. Figure 3 gives a brief overview of 5G slicing.

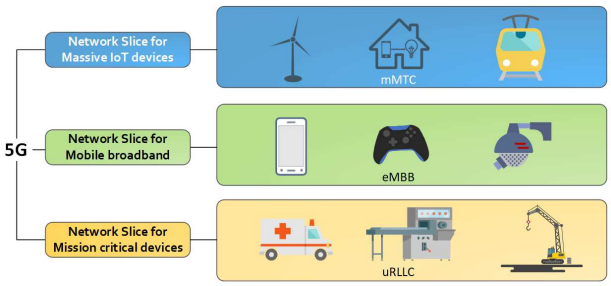

Fig. 3. Network slicing based on user types

D. *SDN backbone*

The incorporation of Software defined networking (SDN) into our primary platform enables us to have minute control over network elements and functionalities. The novel SDN system was conceptualized in the year of 2010 aiming to remove the stringent nature of legacy networks [24] separating the control plane from data plane while providing centralized intelligence for the whole network. It is segmented into three layers: The application layer, control layer and the infrastructure layer [25]. The application layer includes all the user applications, which is linked with the northbound APIs (application programmable interface). These REST APIs (Representational state transfer APIs) connect application layer to the next layer, which is the control layer. The control layer includes the controller of the network that can be a singular controller or multiple internal or external controllers handling all the traffic flows within in the network [27]. The controller acts as the brain of the network and employs policies for different elements in the network. The final layer is the infrastructure layer that is composed of various network devices (Edge nodes, routers, IoTs, sensors etc.). This layer is connected via southbound API that replays configuration information to the SDN controller. One of the popular southbound API is the OpenFlow [24]. Being one of the first open standards of SDN, OpenFlow is still widely used for software defined network orchestration. Figure 4 gives an overview of the architecture of SDN.

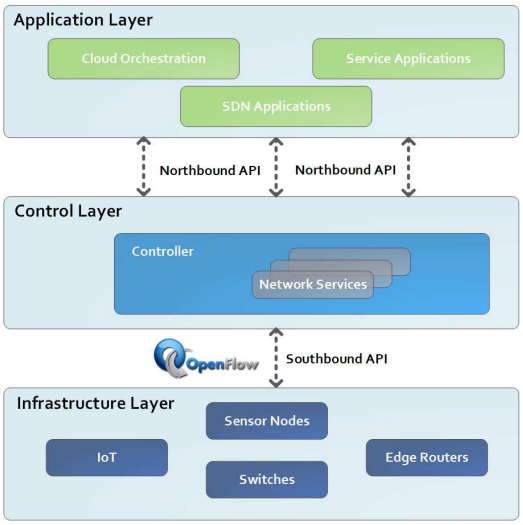

Fig. 4. SDN architecture

E. *Federated Learning*

Standard machine learning models are constrained to centralize training where user data is aggregated to a cloud datacenter. Therefore, it invokes massive security concern as the critical data is being transmitted from user to server. In addition, the data size is also significantly larger therefore demanding more resources and processing delay. On the other hand, a federated learning approach, coined by Google in the year of 2016 [42], is drastically different. In federated learning the model processing is not only loaded on cloud but distributed to different devices. Each device plays a part in generation of the global model in the cloud by generating their own local model and feeding the cloud with its local counterparts. As a result, the cloud does not get overwhelmed with data processing requests from each individual devices as they generate their own models. Additionally, the data sharing utilizes local differential privacy (LDP) techniques, as it is one of the state of the art security

method for statistical data aggregation [28]. There are several federated learning algorithms introduced over past few years such as such as FedAvg [29], FedSGD [30], FedProx [31] and FedDANE [32] etc. For our proposed framework, we have mainly focused on the usage of FedAvg as it is a communication efficient algorithm perfectly suited to work with massive swarms of clients. Our terrestrial backhaul contains separate base stations for individual zones that aggregates all the local models from different IoT devices and performs the global modeling based on aggregated data through LDP.

IV. Proposed Framework

Our proposed framework consists of LEO constellations orbiting the planet, LoRa enabled low power IoT devices and several terrestrial base stations scattered throughout the terrain inside or outside of the space colonies. These base stations are directly connected to the satellite backhaul (as mentioned previously in section III) and employs 5G communication (NB-IoT) for all the connected IoT devices in range.

The base station acts as intelligent communication Hubs that dictates traffic flow, bandwidth segmentation, data encryption and network security. Each base station consists of at least two controllers offering raid 1 (mirroring) capabilities so that when one controller fails another can act as a backup for the system. Therefore, we prefer OpenDaylight controller as it offers flexibility in interfacing external network elements with its Java based platform offering deep integration of OpenStack, OPNFV (Open Platform for Network Function Virtualization) and numerous other cloud platforms. Moreover, it has a model driven approach offered by YANG XML attributes providing network supervision [26]. The system contains a decoy server that works as a shield even if the firewall fails to block malicious mini-streams. A virtual firewall stands at the frontline being the first line of defense filtering and discarding the malicious traffics from the benign ones.

This filtration process is regulated by a machine learning based model, which aggregates traffic data from various IoT devices in the network. This aggregation process is done with federated averaging (FedAvg) taking individual local models of each IoT data streams and sending it to the primary controller on the base stations. Each IoT devices will generate its local model which could be based on popular machine learning models such as Decision Tree (DT), Random Forest, Support Vector Machine (SVM), Deep Learning Neural Networks (NN) etc. Clients will run stochastic gradient descent [33] on their local data for n number of epochs defining their weights and then train local models. These local models are then sent to controller using privacy preserving manner leveraging local differential privacy. The controller then aggregates the data based on client weights and generates its global model. This model dictates the policies based on traffic pattern on hundreds of IoT devices in the network. However, even though initial inferences might potray some minor inaccuracies but as more data is fed by the minutes, the system achieves very high accuracy in malicious traffic prediction just like every other machine learning based models.

In terms of LoRa enabled low power devices, the data is directly sent to the LEO satellites and then forwarded to the base stations. The base stations then perform the necessary AI governing processes then employs policies. We have deliberately avoided a model aggregation point on the satellites to reduce the load and latency, which might be an interesting approach for our future research with empirical implementation. Figure 5 represent our proposed framework.

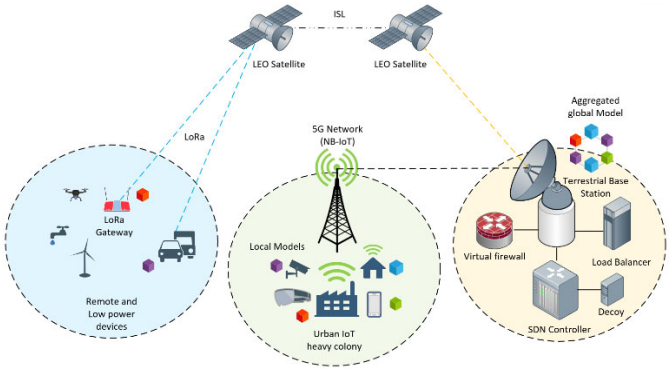

Fig. 5. SDN-FL based Satellite-IoT framework

V. Conclusion and Future Work

IoT ubiquity is the future be it is a terrestrial or an extra-terrestrial network. We can deduce with certainty that it will be a major part of our space colonization ventures. Nevertheless, it is imperative to develop a solid and secured network infrastructure to preserve the ease of access of these devices by ensuring data privacy. With our SDN based FL framework, we have tried to conceptualize this idea by incorporating satellite backhaul with IoT network while utilizing federated learning techniques for preservation data from intrusions and data breach. However, the scope of the project cannot be determined unless empirical data is gathered based on real life giant network infrastructures. For our future work, we hope to achieve that task by incorporating real IoT device variants covering air, ground and underwater and perform rigorous evaluation to gauge the system efficacy. Moreover, we would like to use network slicing to segment terrestrial IoT networks into separate slices having customized 5G technologies such as URLLC, eMBB, nMTC for each slice depending on user types, which ensures QoS depending on data requirements. Additionally, we would like to apply different federated learning techniques to find out the performance differences and efficiency for each of the setups on real life networks.

References

[1] "Perseverance, NASA's newest Mars rover", The Planetary Society, 2022. [Online]. Available: https://www.planetary.org/space-missions/perseverance. [Accessed: 13- Jul- 2022].

[2] G. Kay, "Elon Musk said life on Mars won't be luxurious — it will be 'cramped, difficult, hard work'", Business Insider, 2022. [Online]. Available: https://www.businessinsider.com/elon-musk-mars-trip-cramped-difficult-hard-work-2022-4. [Accessed: 13- Jul- 2022].

[3] J. Liu, Y. Shi, Z. Fadlullah and N. Kato, "Space-Air-Ground Integrated Network: A Survey", IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 2714-2741, 2018.

[4] M. Pan, P. Li and Y. Fang, "Cooperative Communication Aware Link Scheduling for Cognitive Vehicular Networks", IEEE Journal on Selected Areas in Communications, vol. 30, no. 4, pp. 760-768, 2012.

[5] N. Cao, Y. Chen, X. Gu and W. Feng, "Joint Radar-Communication Waveform Designs Using Signals From Multiplexed Users", IEEE Transactions on Communications, vol. 68, no. 8, pp. 5216-5227, 2020.

[6] A. Salam and S. Shah, "Internet of Things in Smart Agriculture: Enabling Technologies", 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), 2019.

[7] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. Stefanizzi and L. Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems", IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515-526, 2015.

[8] M. Mahmud, K. Bates, T. Wood, A. Abdelgawad and K. Yelamarthi, "A complete Internet of Things (IoT) platform for Structural Health Monitoring (SHM)", 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), 2018.

[9] H. Lu, Q. Liu, D. Tian, Y. Li, H. Kim and S. Serikawa, "The Cognitive Internet of Vehicles for Autonomous Driving", IEEE Network, vol. 33, no. 3, pp. 65-73, 2019.

[10] W. Sun, P. Bocchini and B. Davison, "Applications of artificial intelligence for disaster management", Natural Hazards, vol. 103, no. 3, pp. 2631-2689, 2020.

[11] J. Wellington and P. Ramesh, "Role of Internet of Things in disaster management", 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017.

[12] S. Poslad, S. Middleton, F. Chaves, R. Tao, O. Necmioglu and U. Bugel, "A Semantic IoT Early Warning System for Natural Environment Crisis Management", IEEE Transactions on Emerging Topics in Computing, vol. 3, no. 2, pp. 246-257, 2015.

[13] W. Ejaz, M. Azam, S. Saadat, F. Iqbal and A. Hanan, "Unmanned Aerial Vehicles enabled IoT Platform for Disaster Management", Energies, vol. 12, no. 14, p. 2706, 2019.

[14] C. Liu, W. Feng, Y. Chen, C. Wang and N. Ge, "Cell-Free Satellite-UAV Networks for 6G Wide-Area Internet of Things", IEEE Journal on Selected Areas in Communications, vol. 39, no. 4, pp. 1116-1131, 2021.

[15] S. Kim, J. Jeong, M. Hwang and C. Kang, "Development of an IoT-based atmospheric environment monitoring system", 2017 International Conference on Information and Communication Technology Convergence (ICTC), 2017.

[16] J. Matos and O. Postolache, "IoT enabled aquatic drone for environmental monitoring", 2016 International Conference and Exposition on Electrical and Power Engineering (EPE), 2016.

[17] "Cyber Attacks on IoT Devices Are Growing at Alarming Rates | Venafi", Venafi.com, 2022. [Online]. Available: https://www.venafi.com/blog/cyber-attacks-iot-devices-are-growing-alarming-rates-encryption-digest-64. [Accessed: 14- Jul- 2022]

[18] H. Landi, "82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds", fiercehealthcare.com, 2022. [Online]. Available: https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds. [Accessed: 14- Jul- 2022]

[19] M. De Sanctis, E. Cianca, G. Araniti, I. Bisio and R. Prasad, "Satellite Communications Supporting Internet of Remote Things", IEEE Internet of Things Journal, vol. 3, no. 1, pp. 113-123, 2016.

[20] H. Chen, M. Xiao and Z. Pang, "Satellite-Based Computing Networks with Federated Learning", IEEE Wireless Communications, vol. 29, no. 1, pp. 78-84, 2022.

[21] H. McMahan, E. Moore, D. Ramage, S. Hampson and B. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data", in 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017, Fort Lauderdale, Florida, USA, 2017.

[22] O. Flauzac, C. Gonzalez, A. Hachani and F. Nolot, "SDN Based Architecture for IoT and Improvement of the Security", 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, 2015.

[23] G. Yao, J. Bi and L. Guo, "On the cascading failures of multi-controllers in Software Defined Networks", 2013 21st IEEE International Conference on Network Protocols (ICNP), 2013.

[24] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, "OpenFlow", ACM SIGCOMM Computer Communication Review, vol. 38, no. 2, pp. 69-74, 2008.

[25] R. Uddin and M. Monir, "Evaluation of Four SDN Controllers with Firewall Modules", Proceedings of the International Conference on Computing Advancements, 2020.

[26] "What Is YANG? | Tail-f Systems", Tail-f.com, 2022. [Online]. Available: https://www.tail-f.com/what-is-yang/. [Accessed: 14- Jul- 2022]

[27] M. Monir, R. Uddin and D. Pan, "Behavior of NAPT Middleware in an SDN Environment", 2019 4th International Conference on Electrical Information and Communication Technology (EICT), 2019.

[28] S. Truex, L. Liu, K. Chow, M. Gursoy and W. Wei, "LDP-Fed", Proceedings of the Third ACM International Workshop on Edge Systems, Analytics and Networking, 2020.

[29] J. Konecnˇ y, H. McMahan, F. X. Yu, A. Theertha Suresh, D. Bacon and P. Richtarik, "Federated learning: strategies for improving communication", Cornell University, 2017 [Online]. Available: https://arxiv.org/abs/1602.05629. [Accessed: 14- Jul- 2022].

[30] H. McMahan, E. Moore, D. Ramage, S. Hampson and B. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data", in 20th International Conference on Artificial Intelligence and Statistics (AISTATS) 2017, Fort Lauderdale, Florida, USA, 2017.

[31] T. Li, A. Kumar Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar and V. Smith, "Federated Optimization in Heterogeneous Networks", 2018 [Online]. Available: https://arxiv.org/abs/1812.06127. [Accessed: 14- Jul- 2022]

[32] T. Li, A. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar and V. Smithy, "FedDANE: A Federated Newton-Type Method", 2019 53rd Asilomar Conference on Signals, Systems, and Computers, 2019.

[33] L. Bottou, "Large-Scale Machine Learning with Stochastic Gradient Descent", Proceedings of COMPSTAT'2010, pp. 177-186, 2010.

[34] "What is geostationary satellite? - Definition from WhatIs.com", SearchMobileComputing, 2008. [Online]. Available: https://www.techtarget.com/searchmobilecomputing/definition/geostationary-satellite. [Accessed: 18- Jul- 2022].

[35] K. Solutions, "Is MEO Poised for New Growth as Satellite Market Shifts?", Kratosdefense.com, 2022. [Online]. Available: https://www.kratosdefense.com/constellations-podcast/articles/is-meo-poised-for-new-growth-as-satellite-market-shifts. [Accessed: 19- Jul- 2022].

[36] C. Heukelman, "LEO vs. MEO vs. GEO Satellites: What's the Difference? | Symmetry Blog", Symmetry Electronics, 2018. [Online]. Available: https://www.symmetryelectronics.com/blog/leo-vs-meo-vs-geo-satellites-what-s-the-difference-symmetry-blog/. [Accessed: 19- Jul- 2022].

[37] "Network", Iridium Satellite Communications, 2022. [Online]. Available: https://www.iridium.com/network/. [Accessed: 21- Jul- 2022].

[38] M. Hoyhtya et al, "Database-Assisted Spectrum Sharing in Satellite Communications: A Survey", IEEE Access, vol. 5, pp. 25322-25341, 2017.

[39] "L-Band satellite frequency: countless advantages for satellite communication - axessnet", axessnet, 2022. [Online]. Available: https://axessnet.com/en/l-band-satellite-frequency-countless-advantages-for-satellite-communication/. [Accessed: 20- Jul- 2022]

[40] L. Sharma, "NB-IoT for 5G", Advances in Wireless Technologies and Telecommunication, pp. 352-372, 2021.

[41] R. Sinha, Y. Wei and S. Hwang, "A survey on LPWA technology: LoRa and NB-IoT", ICT Express, vol. 3, no. 1, pp. 14-21, 2017.

[42] H. B. McMahan et al., "Federated learning: Strategies for improving communication efficiency," in Proc. 20th Int. Conf. Artif. Intell. Stat. (AISTATS), 2017.

[43] "What Is LoRa?", www.semtech.com, 2022. [Online]. Available: https://www.semtech.com/lora/what-is-lora. [Accessed: 21- Jul- 2022]

[44] J. Fraire, et al.,, "Direct-To-Satellite IoT – A Survey of the State of the Art and Future Research Perspectives", Ad-Hoc, Mobile, and Wireless Networks, pp. 241-258, 2019.