

## **Distributed AI and Blockchain for 6G-Assisted Terrestrial and Non-Terrestrial Networks: Challenges and Future Directions**

Kumar Prabhat, Kumar Randhir, Islam A. K. M. Najmul, Garg Sahil, Kaddoum Georges, Han Zhu

This is a Author's accepted manuscript (AAM) version of a publication  
published by IEEE  
in IEEE Network

**DOI:** 10.1109/MNET.001.2200523

### **Copyright of the original publication:**

© 2023 IEEE

### **Please cite the publication as follows:**

Kumar, P., Kumar, R., Islam, A. K. M. Najmul, Garg, S., Kaddoum, G., Han, Z. (2023). Distributed AI and Blockchain for 6G-Assisted Terrestrial and Non-Terrestrial Networks: Challenges and Future Directions. IEEE Network, vol. 37, no. 2. pp. 70-77. DOI: 10.1109/MNET.001.2200523

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

**This is a parallel published version of an original publication.  
This version can differ from the original published article.**

# Distributed AI and Blockchain for 6G-assisted Terrestrial and Non-Terrestrial Networks: Challenges and Future Directions

Prabhat Kumar, Member, IEEE, Randhir Kumar, Member, IEEE, A. K. M. Najmul Islam, Member, IEEE, Sahil Garg, Member, IEEE, Georges Kaddoum, Member, IEEE, and Zhu Han, Fellow, IEEE

**Abstract**—The integration of Terrestrial and Non-Terrestrial Networks (TNTNs) with the sixth-generation (6G) wireless ecosystem will revolutionize the futuristic communication networks by enabling comprehensive interconnection and quality of service. However, such an integrated network will raise serious security and privacy issues due to the insecure communication among untrusted participating entities over an open unsecured public channel. As a result, the entire ecosystem can be accessed by both legitimate users and adversaries. Distributed AI when integrated with blockchain has a great potential to provide a feasible alternative to solve the security and privacy issues of 6G-assisted TNTNs. As a case study, a distributed AI is first adopted to cooperatively participate in the training process of a global model directly on devices. This approach ensures privacy and security of user data, and also confirms that only valid data is used by smart contracts to execute consensus mechanism. The multiple parallel blockchain are employed to securely and efficiently manage, and share data at each layer of 6G-assisted TNTNs. The efficiency of the proposed framework is demonstrated by numerical findings. Finally, prospective open research issues in employing distributed AI and blockchain for 6G-assisted TNTNs are highlighted.

**Index Terms**—Blockchain, Distributed Artificial Intelligence, Terrestrial and Non-Terrestrial Networks (TNTNs), 6G, Security, Privacy and Intrusion Detection System.

## I. INTRODUCTION

**T**HE Terrestrial Networks (TNs) has proven to be a tremendous success in terms of improving communication speed and Quality of Service (QoS), and is mostly used to deliver services in developed areas and high-density locations. On the other hand, the increasing global communication and escalating development of the Internet of Things (IoT) demands ubiquitous communication coverage for its distributed applications [1]. However, the existing TNs lack the stability, availability, and responsiveness needed for future

IoT applications, and is also vulnerable to natural catastrophes. For example, during natural catastrophes, connection failures may stall or obstruct adequate response, causing considerable damage to business and property, as well as the loss of lives. Furthermore, due to geographical limitations, TNs are unable to cover the huge airspace and marine area [2].

The recent research has been kicked off in academia, and industry to integrate Non-Terrestrial Networks (NTNs) including satellites and Unmanned Aerial Vehicles (UAVs) with current TNs. Since the TNs has deployment and coverage restrictions, the NTNs might be used as a supplement to accomplish worldwide connectivity through satellite constellations [3]. The use of NTNs can assist in the development of a unified wireless system referred as, Terrestrial and Non-Terrestrial Networks (TNTNs), that can be used when TNs are overloaded or out of service during natural catastrophes [4].

In addition to improved and intelligent computing services, the sixth generation (6G) networks will combine new cost-effective technological innovations, enhancing the present TNTNs ecosystem by providing performance that is superior to 5G while also addressing future services and applications [5]. Though 6G-assisted TNTNs have been envisioned as a key enabler for meeting the communication needs of IoT applications, they confront a number of security and privacy issues. This is due to the fact that, the 6G-assisted TNTNs use the same protocols (e.g., TCP/IP) as used by the legacy networks and in IoT settings [6]. Furthermore, due to the communication of participating entities over open and unsecured public channel, the adversaries can also infiltrate the ecosystem to gain unauthorized access to provided resources (e.g., data, services, storage units, and computing units) by simply deploying or compromising existing communicating devices, resulting in critical security issues. For example, denial-of-service (DoS), distributed denial-of-service (DDoS), eavesdropping, exploiting security flaws, and spoofing are some common examples of these attacks [7]. Apart from this, data privacy, and data integrity are another key issues of 6G-assisted TNTNs. We consider Active Data Privacy Attacks (ADPA) and Passive Data Privacy Attacks (PDPA) as the most common types of data privacy attacks [8]. As more devices become accessible and connect to 6G-assisted TNTNs, securing and protecting them from multiple untrustworthy authorities becomes extremely difficult. The research on security and privacy of 6G-assisted TNTNs are still in its early stage. Most of the existing research on these topics

Prabhat Kumar and A. K. M. Najmul Islam are with the Department of Software Engineering, LUT School of Engineering Science, LUT University, 53850 Lappeenranta, Finland (Email: prabhat.kumar@lut.fi, najmul.islam@lut.fi).

Randhir Kumar is with Department of Computer Science and Engineering, SRM University AP, AP 522240, India. (Email: randhir.honeywell@ieee.org).

Sahil Garg is with the Ultra Communications, Montreal, Canada Email: garg.sahil1990@gmail.com

Georges Kaddoum is with the Electrical Engineering Department, École de Technologie Supérieure, Université du Québec, Montréal, QC H3C 1K3, Canada (georges.kaddoum@etsmtl.ca)

Zhu Han is with the Department of Electrical and Computer Engineering at the University of Houston, Houston, TX 77004 USA, and also with the Department of Computer Science and Engineering, Kyung Hee University, Seoul, South Korea, 446-701. E-mail: hanzhu22@gmail.com

TABLE I: A comparison of existing solutions in 6G-assisted TNTNs.

Application	Area	Technology	Network	Security of 6G-assisted TNTNs	Privacy of 6G-assisted TNTNs	Advantage	Limitation
Data routing and security [2]	TNTNs	NA	6G	✓	×	Overview of network architecture	No concrete model
Resource management [4]	TNTNs	NA	6G	×	×	Use cases of 6G and TNTN	Lacks case study
Intrusion Detection System [9]	IoT	Distributed AI/ML	Legacy network	✓	×	High detection rate and accuracy	Model vulnerable to data poisoning attack
Resource management Security [10]	TNTNs	AI	6G	✓	×	Specification of multi-layer NTN	Lacks case study
Data Security [11]	SAG	Blockchain and AI	6G	✓	✓	Improved security	High consensus computation cost
Network security [12]	SAG	Blockchain and AI	NA	✓	✓	Enhanced Security and privacy	Lacks authentication
Intrusion Detection System [13]	IoT	Distributed AI/ML	Legacy network	✓	×	Reduced training time	Model vulnerable to data poisoning attack

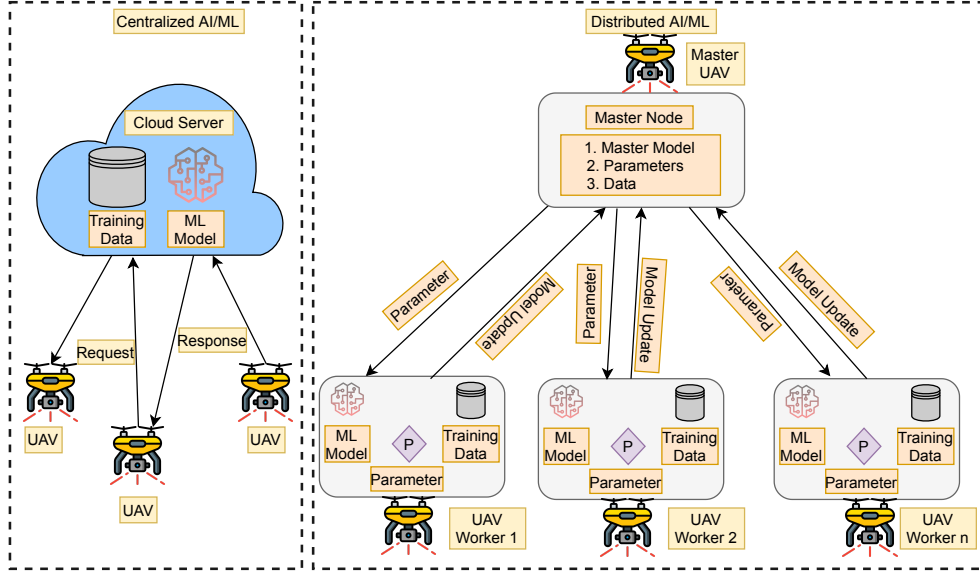


Fig. 1: Centralized versus Distributed AI/ML training.

focuses on IoT networks [13], 5G networks, brief excursions into specialized technologies like Artificial Intelligence and Machine Learning (AI/ML) [9], or scattered ideas in generic surveys regarding 6G concepts [10] and blockchain [11], [12]. A through comparison of existing solution are shown in Table I. It is seen most of the work concentrated on the use of distributed AI/ML or blockchain, while there is limited study on how efficiently we can combine distributed AI/ML with blockchain in 6G-assisted TNTNs environment. Table II refers to the most common notations used in the article.

Motivated from aforementioned challenges and limitations, we propose a distributed AI/ML and blockchain integrated framework to enhance security and privacy in 6G-assisted TNTNs. As more data is created by IoT devices/machines, privacy concerns and data rules may impose restrictions on data movement, distributed AI/ML is specifically employed to enforce local learning. This process efficiently detects intrusion in the network. The valid transactions are further used by the multiple parallel blockchain located at space-air network to store the data. Furthermore, the blockchain method is critical in this type of communication environment since it is tamperproof, anonymous, decentralized, and resistant to many forms of data security and privacy attacks. As a result, a blockchain-based access control and key creation method is proposed for 6G-assisted TNTNs communication.

TABLE II: Most common notations used in the article

Symbol	Explanation
TNTNs	Terrestrial and Non-Terrestrial Networks
UAVs	Unmanned Aerial Vehicles
SC	Smart Contract
ESL	Ephemeral Secret Leakage
IPFS	InterPlanetary File System
PoA	Proof-of-Authority

The blockchain-based approaches presented in the article [12], [11], [8] used blockchain ledger to store the entire transaction, making blockchain quite inefficient and costly. This framework, on the other hand, leverages the InterPlanetary File System (IPFS) as off-chain storage, resulting in lower storage costs, increased scalability, and throughput when accessing 6G-assisted TNTNs data. The numerical results show the effectiveness of the proposed approach. Finally, from the viewpoints of distributed AI/ML, blockchain security, and data utilization, we present an overview on many future research directions.

## II. FUNDAMENTALS OF DISTRIBUTED AI/ML AND MOTIVATION OF BLOCKCHAIN

As we become more captivated with AI decision making, ML in general is finding its way into our everyday lives.

The two most commonly methods, centralized and distributed architectures used to train the AI/ML models are discussed in the following subsections.

#### A. Centralized AI/ML vs Distributed AI/ML

In a typical centralized training architecture, the data generated by IoT devices such as UAVs is sent to the cloud servers, where they are first evaluated, required features are extracted and finally using the high-performance servers of cloud, the model is trained efficiently. The centralized AI/ML scenario on the left-hand side of Fig. 1 illustrates this strategy, in which models may be deployed at cloud and used at scale. During this process a large number of training datasets are obtained due to the interaction between UAV-cloud, and as a result various intelligent AI/ML-based apps are developed. However, the phenomenal performance of AI/ML is achieved at the cost of user privacy. The data shared with cloud can include personally identifiable information (e.g., passport or driving license information), protected health information (e.g., medical and diagnosis records), payment data (e.g., bank and credit card details), and so on. A malicious cloud can leak these critical information, and moreover privacy of users are likely to be jeopardized by eavesdropping attacks [14].

With the growing vulnerabilities of sending data to a centralized entity such as cloud, a demand for real-time intelligence is pushing distributed AI/ML, where training, predictions, and inferences are based on real-time data. To enhance training efficiency, distributed training in AI/ML may be defined as the collaboration across computing resources by partitioning training tasks using parallelized data or models operating on various GPUs / CPUs. In this setting also called as master/slave style, the server distributes a pre-trained or generic model to the participating devices, rather than sending a request for user's private data to the cloud [13]. The following steps need to be performed by computing nodes in order to orchestrate a distributed AI/ML training, as indicated in right side of Fig. 1. Each node starts by calculating local parameters using local data. The nodes then interact with the aggregator(s) in order to obtain a globally aggregated parameter that can be used to update the model. Typically a centralized parameter server also known as the master node aggregates the parameters and sends the aggregated result to each computing node located at different location [9]. Therefore, the data remains with the local devices and only parameters with AI/ML model are shared.

#### B. Motivation of Blockchain

The 6G-assisted TNTNs and its application are data-driven, with enormous amounts of data generated by a variety of end devices and processed to fuel a wide range of applications [9]. The distributed AI/ML based application use the centralized aggregator to run specific model and verify the dataset. However, the centralized storage and administration functionality in AI/ML systems may expose data to security risks (e.g., theft or malicious alteration as a result of server breach), resulting in privacy violations and network disruption. Since this legitimacy of source data cannot be verified, AI

systems may be prone to making inaccurate decisions [13]. Moreover, the communication between different layers of 6G-assisted TNTNs is performed over open insecure wireless medium. As a result, malicious users in this communication may launch a variety of attacks, including DoS attacks, DDoS attacks, replay, man-in-the-middle attacks, packet spoofing attacks, and Ephemeral Secret Leakage (ESL) attacks, and so on. Therefore, there is an urgent need of a security protocol that should be sufficiently safe enough to withstand the aforementioned attacks against an adversary in the 6G-assisted TNTNs environment [11]. Blockchain technology has the potential to advance the 6G-assisted TNTNs paradigm by offering a trustworthy shared ledger and decentralized computing capabilities for secure data sharing, where the recorded cryptographic information (e.g., signature or hash value) of digital asset, device information, processed or sensory data can be reliable, traceable, undeniable and immutable [6]. Specifically, blockchain is a decentralized, open ledger that uses cryptography to effectively and permanently record transactions between two parties. The failure of one node has no impact on the system, and the intelligent functioning of the trusted code is supported by other participating nodes and smart contracts [8]. Blockchain, when used with 6G-assisted TNTNs will offer a decentralized control without the need for a single authority to set the rules. To evaluate the reliability of information sources and avoid data fabrication, blockchain might be used to record the trust, configuration, and registration information of devices as transactions in blocks [11]. As a result, a secure and decentralized data exchange mechanism, without a trusted third entity or middleman is essential, and blockchain has the ability to meet all of the aforementioned requirements for 6G-assisted TNTNs.

1) *Consensus mechanism*: Since there are no central authority on the blockchain, it is critical to verify that the ledgers agreed upon by all participating entities are equal and consistent. The consensus protocol is the backbone of blockchain-based 6G-assisted TNTNs, determining block time, security, scalability, and consistency [12]. The block proposal, block propagation, block audit, synchronization, and incentives are the fundamental components, and should be included in any blockchain consensus mechanism. There are several sorts of existing common ways for building consensus in blockchain such as Proof of work (PoW), Proof of Stake (PoS), Proof of X (PoX) series, Byzantine fault tolerance (BFT) series [8].

2) *Smart Contract*: The application of distributed ledger technology has been expanded with smart contracts. Two of its most essential characteristics are the execution of smart contracts in the peer-to-peer mode without the involvement of a centralized third party and the provision of services without any centralized dependency. Each SC's execution is documented as a transaction and is comprised of the four phases: creation, deployment, execution and completion. Contracts are also smarter than paper contracts since they execute themselves based on predetermined conditions [13].

### III. 6G-ENABLED TNTNS ARCHITECTURE

In this section, we show a possible 6G-assisted TNTNs design, which is a three-tier integrated space-air-ground and

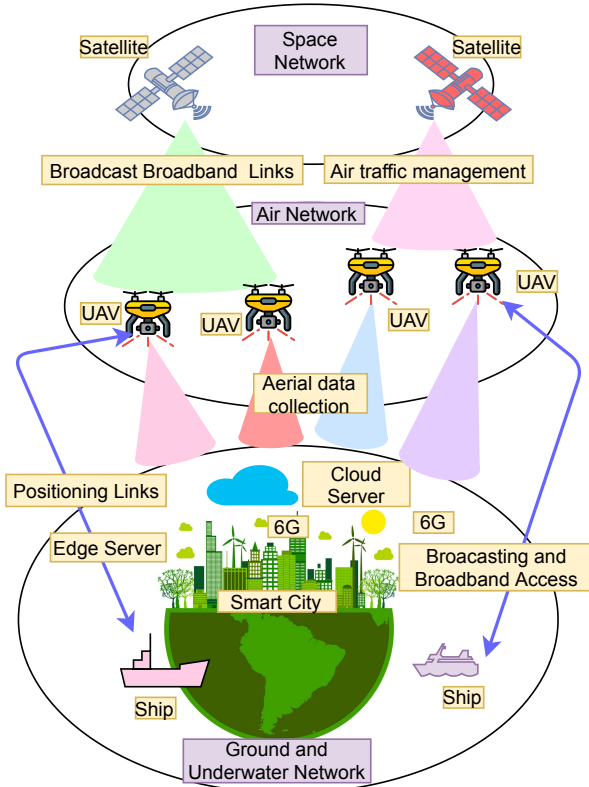


Fig. 2: The architecture of 6G-assisted TNTNs.

underwater network, as illustrated in Fig. 2. Instead of fibre optics and base stations, the 6G uses satellite-based communication system, with satellite launch and deployment taking place mostly in orbit [11]. Moreover, to provide services worldwide, the satellite communication is crucial in 6G [1]. As a consequence, 6G networks may provide consumers flexible and limitless space communication options [2]. A brief discussion about these sub-networks are listed below.

#### A. Space Network

The space network is made up of a collection of satellites as well as the associated terrestrial infrastructure, such as ground stations and Network Management and Control Centres (NOCCs). Communication satellites are classified into three orbital altitudes: low Earth orbit (LEO) is at the altitude of 500–2,000 km, medium Earth orbit (MEO) is at the altitude of 2,000–36,000 km, and high geostationary Earth orbit (GEO) is above the altitude of 36,000 km. Satellite networks are characterized as broadband or narrowband based on channel bandwidth [12]. Broadband satellite networks may deliver a high-speed data rate of 10 Gbps and are predicted to reach 1000 Gb/s capacity by 2022, whereas narrowband satellite systems can mostly deliver consumers with worldwide telephony and low-rate data services [2]. In addition, several services, such as emergency rescue, earth observation and navigation, SpaceX and so on, are available using the satellite network’s global coverage [11].

#### B. Air Network

The air network includes low altitude platforms (LAPs) and high-altitude platforms (HAPs). Various aircraft platforms, such as UAVs, balloons, and airships, are limited to varying operational altitudes due to size, weight, and power limits [4]. The air network has minimal costs, is easy to construct, and has a large coverage area, making it suitable for providing regional wireless access services [10].

#### C. Ground and Underwater Network

To support a range of services, the ground network is made up of a variety of heterogeneous communication systems, such as mobile ad hoc network (MANET), cellular network, wireless local area network (WLAN), and so on. When combined with the aforementioned technologies, 6G has the potential to give worldwide coverage. Additionally, user services will be faster, and smart phones will be able to connect directly and quickly with one another [12]. An underwater network can provide communication services for both deep-sea and wide-sea operations, facilitating the construction of an ocean surveillance system [11].

### IV. CASE STUDY OF THE DISTRIBUTED AI/ML AND BLOCKCHAIN FOR 6G-ASSISTED TNTNS ARCHITECTURE

In this section, based on 6G-assisted TNTNs ecosystem, we show how distributed AI/ML and blockchain can be used to enhance its security. We take advantage of distributed AI/ML to create an intrusion detection system based on which the smart contracts employ the legal transactions to operate the consensus mechanism. The transactions are stored in IPFS once consensus is attained, and the generated hash is recorded in the blockchain ledger.

#### A. System Model

The proposed framework for enhancing security in 6G-assisted TNTNs is shown in Fig. 3. It consists of three sub-networks, the ground, the air and the space and has IoT devices, UAVs, satellite and Trusted Authority (TA) as the main participating entities. The TA is in charge of key secret maintenance, which may be used to validate authentic registration identities for participating entities without exposing their personal information. The blockchain network is integrated only with the air and space environment, and both sub-network maintain their own distributed ledger technology. The proposed IDS using distributed AI/ML is used by both sub-networks to identify valid transactions, based on which smart contracts are executed. Moreover, the ground sub-network includes various IoT devices/machines located at different geographical locations with low computational power. The air sub-network includes UAVs and other aerial objects used to collect the real time data from IoT devices, and has powerful computing ability used to execute consensus mechanism and distributed AI/ML-based IDS. The space network includes various moving satellites used to provide large communication coverage including air traffic management, broadcast broadband links, weather forecasting, and so on. When blockchain

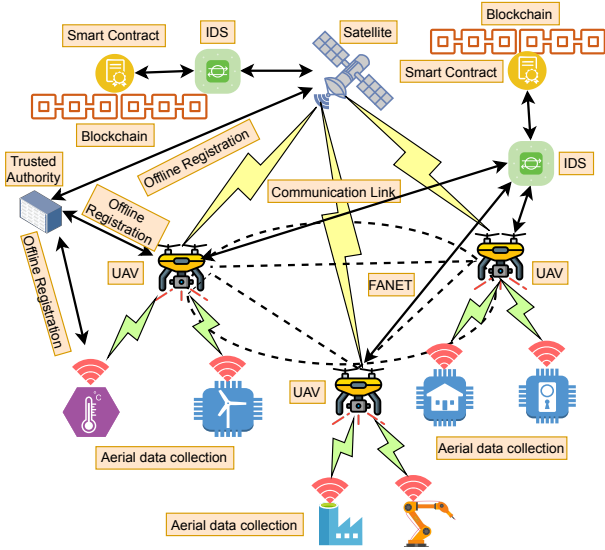


Fig. 3: Proposed framework for 6G-assisted TNTNs.

is applied to satellite networks, the massive amount of client requests may exceed the bandwidth-limitation and extremely mobile satellite connections, making scalability the most difficult obstacle. Therefore, IPFS is used to store entire transaction and returned hash is stored in blockchain ledger. This mechanism ensures data to be transparent, auditable, immutable and traceable.

### B. Threat Model

For our proposed framework in 6G-assisted TNTNs, we leverage the widely known Dolev-Yao (DY) adversary model. The participating entities communicate on a public media, which is vulnerable to eavesdropping and other cyber threats, according to the DY model. In this communication, satellites, UAVs and IoT devices cannot be trusted. As a result, the communications sent out may be delayed, updated, dropped, or changed. Furthermore, in the 6G-assisted TNTNs environment, the TA is a completely trusted network entity. In addition, we follow the principles of the Canetti and Krawczyk's (CK) adversary model. According to the CK-adversary model, an adversary has access to all of the features given by the DY model, as well as additional capabilities such compromising secret credentials via session hijacking assaults.

### C. Proposed Distributed AI/ML and Blockchain Framework

In this subsection, we discuss the proposed framework and its two major components: (1) distributed AI/ML to detect intrusion and (2) blockchain for secure data sharing.

1) *Distributed AI/ML for Intrusion Detection*: The proposed IDS is based on three key main modules: traffic processing module, intrusion detection module, and transaction handling module. All these steps are hosted locally, i.e., at UAV and at satellite. The traffic processing module is responsible to convert categorical values into numeric, then the obtained data is normalized, and finally features are selected using mutual-information technique [13]. Then the data is feed into intrusion

detection module to classify normal and attack transactions. In this step, the parallel and distributed processing of multiple IoT data takes place to reduce learning and inferencing time. As a result, we propose an unique distributed AI/ML technique for analyzing and detecting intrusions in 6G-assisted TNTNs traffic. As depicted in Fig. 1, the IDS consist two nodes master and worker. First the master node is in charge of global learning. The second type is the worker node that does local learning. The centralized cloud computing-based forensics methodology suffers from scalability issues; however this distributed computation solves that problem. The outputs of the distributed AI/ML (at worker nodes) are sent and kept at the master node, where they are used to identify intrusions in freshly created and unidentified IoT traffic samples. As a result, our distributed learning architecture permits obtaining the appropriate AI/ML training parameters, and hence avoids overfitting. In order to train the IDS, we have used XGBoost and random forest, and then trained and tested them in distributed manner using algorithm mentioned in [9]. Finally, the transaction handling module is responsible to maintain the log of intrusion, where the global state of participating devices are updated. The valid transactions are used by the blockchain module to enforce secure data sharing.

2) *Blockchain for Secure Data Sharing*: To enable secure sharing and communication between participating entities, authentication schemes plays the major role. The authentication schemes is checked during the data sharing between two different entities. The entire process is bounded with the entities registrations and its authentication process. In proposed model, session based authentication takes place between IoT device and UAV, UAV to UAV data sharing, UAV to satellite (SAT) sharing and SAT to SAT data sharing. The secure data sharing between these components is performed with public key cryptographic approach. Registration process includes UAV identity, i.e., MAC address, temporary key, pseudo identity, and timestamp. Next, based on the above parameters private and public key is computed. While forwarding the data between UAVs, public key of receiving UAV is used and data gets encrypted. Similarly, while data forwarding from UAV to SAT, UAV uses SAT public key to encrypt the data. Further, communication between SAT to SAT is performed, and public key of receiving SAT is used for data encryption. To perform all these operation, smart contracts-based blockchain authentication scheme is applied in the proposed model.

### D. Illustrative Results

The research is being carried out on the Tyrone PC, which has a 2 GHz Intel(R) Xeon(R) Silver 4114 CPU, 128 GB of RAM, and a 2 TB hard drive. The H2O.ai platform and Kubernetes are used to train and test the distributed AI/ML models. Python programming language is used to run the implementation methods. The Ethereum Ropsten Test network is used for the blockchain experiment. The smart contracts are written in version of Solidity (0.8.13). Metamask is started in the browser in order to allow the Ropsten Test network. Different evaluation metrics such as ACcuracy (AC), Precision (PR), Detection Rate (DR) and F1 score are used to thoroughly

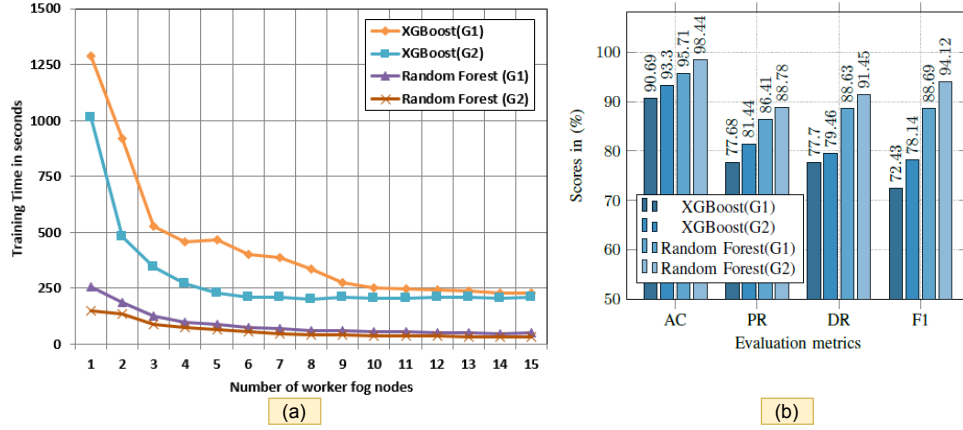


Fig. 4: Distributed AI/ML results

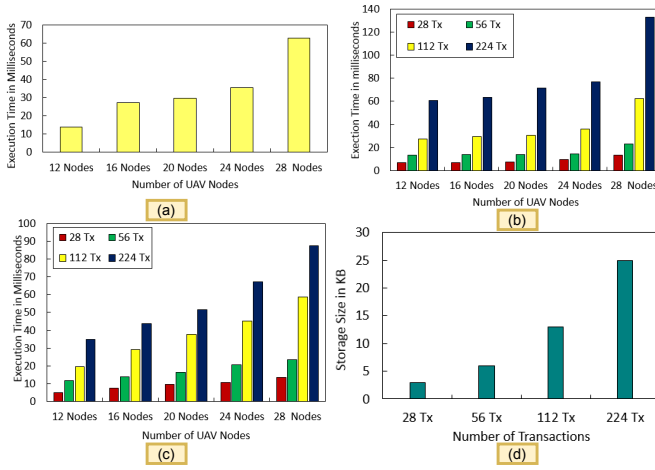


Fig. 5: Blockchain results

evaluate the IDS performance [9]. The ToN-IoT dataset is used to validate the performance of the proposed approach. In this experiment full features dataset is referred as G1 and 20 features selected using mutual-information technique is referred as G2. In the left side of Fig. 4, we have shown the scalability of the proposed approach. It is seen that the experiments are conducted on 15 worker nodes, resulting in decrease training time. It is worth noting that after 10 worker nodes, increasing the worker nodes had no effect on both distributed techniques but overall random forest takes less time compared to XGBoost. The performance of distributed XGBoost and Random Forest in terms of AC, PR, DR and F1 score is shown in the right side of Fig. 4. It is seen that both approach based on G2 has performed well compared to G1 but random forest has achieved highest numerical values using G2 dataset for all above metrics. Fig. 5 shows result analysis of blockchain network. It includes transaction upload time, block mining time, block creation time, and off-chain storage size. To make the network more scalable IPFS based off-chain storage is used. The results shows transaction upload time and its off-chain storage size (in KB). The transactions upload time is evaluated on varying number of peers over the network. To verify the transactions in network a smart contracts based

Proof-of-Authority (PoA) consensus mechanism is applied. In the present study of blockchain analysis, all evaluation has been carried out for the UAVs.

## V. OPEN ISSUES AND CHALLENGES

Distributed AI/ML and blockchain is thriving ecosystem with a numerous potentials to enrich 6G-assisted TNTNs. With a bright future ahead, there are still various hurdles that requires significant research efforts to cope with the following challenges.

### A. Fault Tolerance

Synchronous parallel approaches appear to scale much better than parameter server alternatives (up to a particular cluster size), but they lack fault tolerance: If a single machine fails, the entire training process is halted. At a certain number of nodes, the likelihood of any node going down becomes sufficiently high to cause near-constant stalling. Typical implementations of these high-performance computing-inspired paradigms, such as message passing interface and NVIDIA Collective Communications Library, lacks fault-intolerant [8]. It would be interesting to investigate whether there is a more efficient method to build the fault-tolerant synchronous parallel approach.

### B. Closing the Gap Between Simulation and Real-World Scenarios

Simulated training gives data at a minimal cost, but there are inherent inconsistencies with real-world conditions. Bridging the simulation-reality gap necessitates approaches that can account for mismatch in both sensing and actuation i.e., the simulator needs to be more precise and should be verifiable in 6G-assisted TNTNs dynamics [15]. However, the challenge might be viewed as broader in the sensing section, since it also contains the more general AI/ML problem of dealing with circumstances in the actual world that do not arise in the simulation.

### C. Throughput and Scalability

Blockchain has evolved into a platform for decentralized applications as a distributed and public transaction database. Despite its growing popularity, blockchain technology has a scalability issue: throughput does not expand as the network grows larger. As a result, scalable blockchain protocols that can address scalability challenges remain in high demand. The scalability of blockchain has been addressed in a variety of ways, including Off-chain, DAG, and Sharding approaches [15], [9]. However, scalability has been hampered by two roadblocks. The first is the poor throughput, and the second is the demand that every node reproduce the full blockchain network's communication, storage, and state representation. Therefore, it is still an open issue to balance the poor parallel structure throughput and scalability of network and data in future blockchain-based solutions.

### D. Smart Contract Security

Smart contracts are becoming increasingly widely used as a digitized agent in distributed systems. To minimize unneeded losses and harmful attacks, smart contracts' security should be maintained. To verify and ensure the accuracy and non-vulnerability of smart contracts, a number of analytical techniques have been built. However, the potential danger may be considerably raised when the code executes in a dispersed network setting of 6G-assisted TNTNs [11]. As a result, figuring out how to include a more secure method into the blockchain has become a top priority.

### E. Blockchain Interoperability

It is critical to overcome the interoperability issues in order to fully realize the potential of blockchain technology in 6G-assisted TNTNs. Interoperability is critical for allowing various blockchain networks to communicate with one another. Although the lack of standards in blockchain benefits developers, it creates significant communication issues owing to the lack of interoperability. The availability of various blockchain networks with diverse consensus models, transaction processes, and smart contract functionality is a big barrier to interoperability. For example, Github has over 6,500 active blockchain projects that use a variety of platforms, programming languages, consensus processes, protocols, and privacy features [11]. As a result, standardization is necessary for business cooperation on application development in order to share blockchain-based solutions and connect them with current systems.

## VI. CONCLUSION

In this article, we investigated the use of distributed AI/ML and blockchain to enhance security and privacy in 6G-assisted terrestrial and non-terrestrial networks. We first discussed the fundamental concept and motivation of distributed AI/ML and blockchain. Then we introduced the architecture of 6G-assisted TNTNs. Furthermore, using a case study, we have comprehensively discussed the growing focus on security and privacy in 6G-assisted TNTNs. Experimental results illustrated

the effectiveness of the proposed framework against various attack and resistance towards different privacy attacks. In addition, we have identified a number of possible future study directions. We believe that this research will encourage more people from academia and industry to investigate the application of security and privacy in 6G-assisted TNTNs, as well as contribute to the development of distributed AI/ML and blockchain technologies in future applications.

### ACKNOWLEDGEMENT

This work is partially supported by NSF CNS-2107216, CNS-2128368, CMMI-2222810, Toyota and Amazon.

### REFERENCES

- [1] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," *IEEE Network*, vol. 35, no. 2, pp. 244–251, 2021.
- [2] X. Zhu and C. Jiang, "Integrated satellite-terrestrial networks toward 6g: Architectures, applications, and challenges," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 437–461, 2022.
- [3] C. Liu, W. Feng, X. Tao, and N. Ge, "Mec-empowered non-terrestrial network for 6g wide-area time-sensitive internet of things," *arXiv preprint arXiv:2103.11907*, 2021.
- [4] G. Araniti, A. Iera, S. Pizzi, and F. Rinaldi, "Toward 6g non-terrestrial networks," *IEEE Network*, vol. 36, no. 1, pp. 113–120, 2022.
- [5] C. L. Stergiou, A. P. Plageras, K. E. Psannis, and B. B. Gupta, "Secure machine learning scenario from big data in cloud computing via internet of things network," pp. 525–554, 2020.
- [6] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "Iot-based big data secure management in the fog over a 6g wireless network," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5164–5171, 2020.
- [7] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6g: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021.
- [8] Y. Wang, Z. Su, J. Ni, N. Zhang, and X. Shen, "Blockchain-empowered space-air-ground integrated networks: Opportunities, challenges, and solutions," *IEEE Communications Surveys Tutorials*, vol. 24, no. 1, pp. 160–209, 2022.
- [9] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect ddos attacks in blockchain-enabled iot network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, 2022.
- [10] S. Kota and G. Giambene, "6g integrated non-terrestrial networks: Emerging technologies and challenges," in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2021, pp. 1–6.
- [11] W. Li, Z. Su, R. Li, K. Zhang, and Y. Wang, "Blockchain-based data security for artificial intelligence applications in 6g networks," *IEEE Network*, vol. 34, no. 6, pp. 31–37, 2020.
- [12] W. Sun, L. Wang, P. Wang, and Y. Zhang, "Collaborative blockchain for space-air-ground integrated networks," *IEEE Wireless Communications*, vol. 27, no. 6, pp. 82–89, 2020.
- [13] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, "A distributed framework for detecting ddos attacks in smart contract-based blockchain-iot systems by leveraging fog computing," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, p. e4112, 2021.
- [14] C. L. Stergiou, K. E. Psannis, and B. B. Gupta, "Infemo: flexible big data management through a federated cloud system," *ACM Transactions on Internet Technology (TOIT)*, vol. 22, no. 2, pp. 1–22, 2021.
- [15] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & iot," *Sustainable Computing: Informatics and Systems*, vol. 19, pp. 174–184, 2018.

**Prabhat Kumar** received his Ph.D. degree in Information Technology, National Institute of Technology Raipur, Raipur, India, under the prestigious fellowship of Ministry of Human Resource and Development (MHRD) funded

by the Government of India in 2022. He is currently working as Post-Doctoral Researcher with the Department of Software Engineering, LUT University, Lappeenranta, Finland. He has many research contributions in the area of Machine Learning, Deep Learning, Federated Learning, Big Data Analytics, Cybersecurity, Blockchain, Cloud Computing, Internet of Things and Software Defined Networking. He is also an IEEE Member.

**Randhir Kumar** received his Ph.D. degree in Information Technology, National Institute of Technology Raipur, Raipur, India in 2021. He is currently working as Assistant Professor with Department of Computer Science and Engineering, SRM University AP, India. Before joining SRM university, he worked as a Post-Doctoral Researcher with the Department of Electrical Engineering, Indian Institute of Technology Hyderabad, India. He has published more than 40 research article in the reputed journals and conferences. His research interest includes cryptographic techniques, information security, blockchain technology, and web mining. He is also an IEEE Member.

**A. K. M. Najmul Islam** is an Associate Professor at Software Engineering, LUT University, Finland. He is an adjunct professor of Information Systems at Tampere University, Finland. He has received his PhD from the University of Turku, Finland, and M.Sc. from Tampere University of Technology, Finland. He has published in other highly ranked journals such as IEEE Transactions on Industrial Informatics (TII), IEEE Transactions on Artificial Intelligence, IEEE Access, Computers in Industry, Computers Education, Journal of Strategic Information Systems, European Journal of Information Systems and Information Systems Journal, Technological Forecasting and Social Change, International Journal of Information Management, Information Technology People, Computers in Human Behavior, Internet Research, Communications of the AIS, among others. He is currently serving as a Senior Editor for Information Technology & People journal.

**Sahil Garg** is currently an AI/ML architect at Ultra Communications, Montreal, Canada. Prior to this, he worked as a Research Professional at Resilient Machine Learning Institute (ReMI), Montreal; Postdoctoral Research Fellow at ÉTS, Montreal; and as a MITACS Researcher at Ericsson, Montreal. He has contributed much research in the areas of machine learning, big data analytics, security and privacy, the Internet of Things, and cloud computing. He has over 90 publications in highly ranked journals and conferences, including 60+ top-tier journal papers and 30+ reputed conference articles. He has been awarded the 2022 IEEE HITC Early Career Researcher Award; 2021 IEEE Systems Journal Best Paper Award; the 2020 IEEE TCSC Award for Excellence in Scalable Computing (Early Career Researcher), the IEEE ICC best paper award in 2018 at Kansas City, Missouri, etc. He is currently a Managing Editor of Springer's Human-Centric Computing and Information Sciences journal. He is also an Associate Editor of IEEE Transactions on Intelligent Transportation Systems, Elsevier's Applied Soft Computing, and Wiley's International Journal on Communication Systems. Dr. Garg also served as an Associate Editor for other reputed journals like Elsevier's Future Generation Computer Systems, IEEE Network Magazine and IEEE Systems Journal. In addition, he also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications.

**Georges Kaddoum** received his Bachelor's degree in electrical engineering from the Ecole Nationale Supérieure de Techniques Avancées, France, his M.Sc. degree in telecommunications and signal processing from Telecom Bretagne, Brest, in 2005, and his Ph.D. degree in signal processing and telecommunications from the National Institute of Applied Sciences, Toulouse, France, in 2009. He is currently an associate professor and Tier 2 Canada Research Chair with ÉTS. His recent research activities cover wireless communication networks, resource allocations, security and space communications, and navigation. He was awarded the ÉTS Research Chair in physical layer security for wireless networks in 2014 and the prestigious Tier 2 Canada Research Chair in wireless IoT networks in 2019. He has published over 150+ journal and conference papers, and has two pending patents. In addition, he received the Research Excellence Award of the Université du Québec in 2018. In 2019, and he received the Research Excellence Award from ÉTS in recognition of his outstanding research outcomes.

**Zhu Han** (S'01–M'04–SM'09–F'14) received the B.S. degree in electronic engineering from Tsinghua University, in 1997, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of Maryland, College Park, in 1999 and 2003, respectively.

From 2000 to 2002, he was an RD Engineer of JDSU, Germantown, Maryland. From 2003 to 2006, he was a Research Associate at the University of Maryland. From 2006 to 2008, he was an assistant professor at Boise State University, Idaho. Currently, he is a John and Rebecca Moores Professor in the Electrical and Computer Engineering Department as well as in the Computer Science Department at the University of Houston, Texas. Dr. Han's main research targets on the novel game-theory related concepts critical to enabling efficient and distributive use of wireless networks with limited resources. His other research interests include wireless resource allocation and management, wireless communications and networking, quantum computing, data science, smart grid, security and privacy. Dr. Han received an NSF Career Award in 2010, the Fred W. Ellersick Prize of the IEEE Communication Society in 2011, the EURASIP Best Paper Award for the Journal on Advances in Signal Processing in 2015, IEEE Leonard G. Abraham Prize in the field of Communications Systems (best paper award in IEEE JSAC) in 2016, and several best paper awards in IEEE conferences. Dr. Han was an IEEE Communications Society Distinguished Lecturer from 2015-2018, AAAS fellow since 2019, and ACM distinguished Member since 2019. Dr. Han is a 1% highly cited researcher since 2017 according to Web of Science. Dr. Han is also the winner of the 2021 IEEE Kiyo Tomiyasu Award, for outstanding early to mid-career contributions to technologies holding the promise of innovative applications, with the following citation: "for contributions to game theory and distributed management of autonomous communication networks."