EasyChair Preprint

№ 11303

# Current 5G Federation Trends: a Literature Review

Andrew Fox, Hisham Kholidy and Ibrahim Almazyad



November 16, 2023

# Current 5G Federation Trends: A Literature Review

Andrew Fox
*Department of Network and Computer Security, College of Engineering, SUNY Polytechnic Institute, Utica, NY, USA.*
*E-mail: foxaj3@sunypoly.edu*

Hisham A. Kholidy, *Senior Member, IEEE*
*Department of Network and Computer Security, College of Engineering, SUNY Polytechnic Institute, Utica, NY, USA. E-mail: kholidh@sunypoly.edu*

Ibrahim Almazyad
*Department of Electrical and Computer Engineering, University of Arizona, Tucson, 85719, AZ, USA.*
*E-mail:almazyad@arizona.edu*

Abstract – 5G is the latest generation of mobile networks, developed with the purpose of faster communication, more spectrum use, and lower latency. With 5G in such high demand, the need for specific services for customers is essential. The federation of 5G services and resources refers to service providers working together to orchestrate services across many domains. Not only will customers have their networking needs met, but it also allows for opportunities for improving services. There are many suggestions on how to improve federation for 5G, which includes implementing technologies like blockchain and Machine Learning (ML). These technologies contain features that could improve the security, speed, and efficiency of the federation process. This paper presents a comprehensive review of the federation of 5G services and resources, the federation process, enabling technologies, such as blockchain and ML, and potential challenges. Additionally, this paper includes a discussion on recent work and future directions for improving federation.

*Keywords – 5G, service federation, resource federation, security, network slicing, blockchain, machine learning*

## I. Introduction

Throughout the history of mobile networks, new demands for faster performance, increased availability, and efficient energy use have expanded to something that was seen as impossible. With this rate of growth comes the need for more advanced communication tools and techniques to fulfill consumer needs. For instance, network slicing, which provisions hardware network functions into standardized software, is utilized to provide a ubiquitous platform that can be used in a variety of ways. Advanced communication can be achieved through network slicing with its ability to create network pods, tailored for specific roles, that match customers' specific needs.

One of the most important techniques used to match advanced communication demands is service and resource federation. Federation allows users to utilize different resources from Administrative Domains (ADs) based on their needs. This allows service providers to offer services and resources to match users' demands.

Although these custom services help customers and the mobile network industry, there are potential issues to consider. With the need for specialized and diverse services, it may be difficult to manage and control the federation of all these resources. Finding a way to organize these resources while protecting customers' privacy and isolating each specialized service to ensure the best cybersecurity practices. Another issue involves devices and/or domains each having different

configurations, which could be a data privacy issue. In technology, devices and domains are often configured in diverse ways, with a wide range of protocols and configurations. Using diverse communication protocols and standards makes 5G federation more complicated and less secure.

Research has been conducted in recent years to find ways to improve the federation process and different applications have been proposed. These proposals use blockchain, Machine Learning (ML), and other novel techniques as solutions to potential security and management concerns with 5G federation. Both blockchain and ML offer unique features, such as encryption and automated actions, that could help improve the way 5G resources are federated.

This paper's main contribution will be the analysis of recent literature work related to the federation of services, highlighting the ideas and concerns related to 5G. It also provides an overview of blockchain and ML technologies, that can assist in improving the federation process. Since these technologies are essential to understanding federation, it is crucial to highlight how they all connect to form this concept. The contributions of our paper are listed below:

- Review of 5G and federation: The background of 5G, the federation of services and resources, and an introduction to the technologies that can be used within the federation process.
- Discuss key concepts related to federation: Analyze the steps and components involved in federating services and resources.
- Highlight the challenges related to service federation and the technologies used with it: Identify and discuss the open issues with the federation of 5G services and resources.
- Experimentation with AI-enabled mobile network: Experiment with 5G AI network traffic in normal and extreme conditions.
- Future research directions: Based on our findings, we have provided potential and relevant challenges that must be researched further. This will help with future 5G developments, along with the technologies that help with the federation process.

Section II provides background information about what 5G is and the federation process. Section III presents a literature review on the key applications of blockchain and ML to improve federation. Section IV provides a discussion on the lessons learned throughout recent publications and future opportunities for service and resource federation in 5G.

## II. Background

5G is the fifth generation of mobile networks, intending to provide more availability, reliability, and lower latency than previous generations. 5G can support a 100x traffic increase compared to 4G, data rates of over 100 Megabits-per-second (Mbps), and utilizes Millimeter waves for better spectrum use [4]. With the demand for fast connections growing, 5G was a massive milestone for wireless communications. Although it has many improvements compared to 4G, some cybersecurity issues have yet to be resolved.

An important concept in 5G for providing specific needs for customers is federation. 5G federation is when services and resources are orchestrated across various Administrative Domains (ADs) [1]. This topic is important for 5G because it allows customers to request specific needs for their network that may be distinct compared to requests from other customers. The federation of

services and/or resources allows service providers to either provide services and/or resources to their customers or to collaborate with other providers to extend services, which helps expand the capabilities of 5G. For example, when a cell tower is overwhelmed by too much traffic, a neighboring cell tower can help offload this traffic so users can still use the services they need. When multi-vendor and commercial service providers, such as AT&T and Verizon, work together in federating services, there are potential opportunities for further research and developments in improving 5G  The goal of 5G is to provide end users with the best data rates and services that meet their needs, which is why the federation of 5G services is necessary.

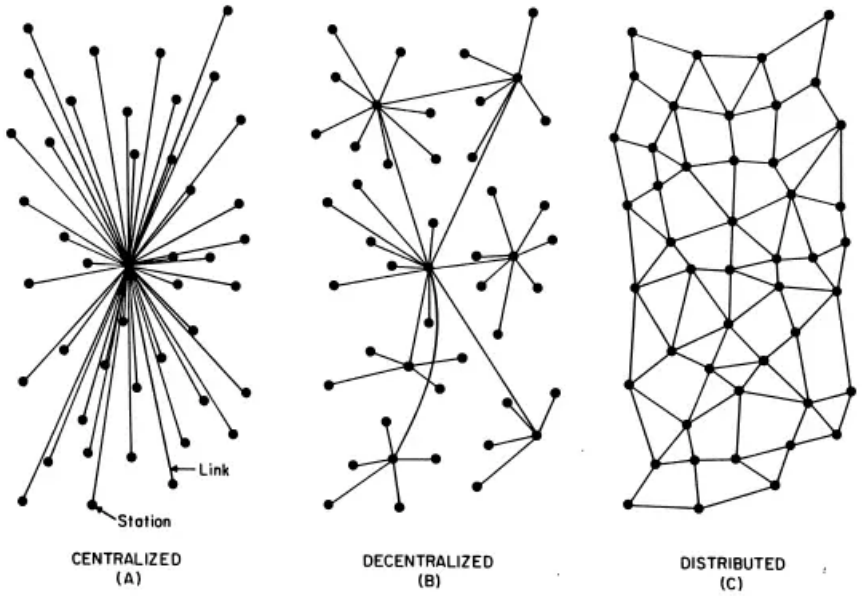


*Figure 1: Centralized, decentralized, and distributed network models comparison [9].*

Federation interactions in 5G can be done in a variety of ways, which include centralized, decentralized, or distributed. Centralized solutions have a single entity that all ADs trust. This entity moderates federation interaction, and all participating ADs trust this single mediator. The solution is scalable and trusted but is a single point of failure and requires persistent servicing. Decentralized solutions have peer-to-peer connections established with each external AD. For these connections to happen, it takes time for each connection to establish a business agreement. The solution does not have the risk of a single point of failure due to the connectivity between every AD but requires more time to configure and has the lowest scalability out of all the interaction solutions. A distributed solution is like a centralized solution, but the central entity is distributed to each AD. It's a hybrid approach with the same benefits as centralized, except it no longer has a single point of failure. Figure 1 reveals the models for the centralized, decentralized, and distributed solutions, and illustrates how the ADs are connected in different ways.

All the discussed solutions follow a procedure, starting with registration and ending with a service or resource deployed. Establishing a peer-to-peer connection or registering with a central entity is the first step of this process. After completing registration, the discovery process begins with the ADs exchanging details of what services and/or resources they can provide. Once it is decided that a part of their services and resources can be federated, an announcement with its offer

is sent to all potential providers. The announcement contains a detailed explanation of what they need. Once the announcement is obtained, the potential providers determine whether they have the required services and/or resources or not. If an AD can meet those requirements, they respond with the pricing of the service. Once the customer receives offers from multiple ADs, they reply to the offer that best meets their needs. The provider then starts to deploy the federated service and resources. Once it is deployed, the provider sends the customer information on usage and the charging procedure, in which the provider will begin charging for the federated service until the customer terminates it. The discussed sequence of communications in the federation process is illustrated in Figure 2.

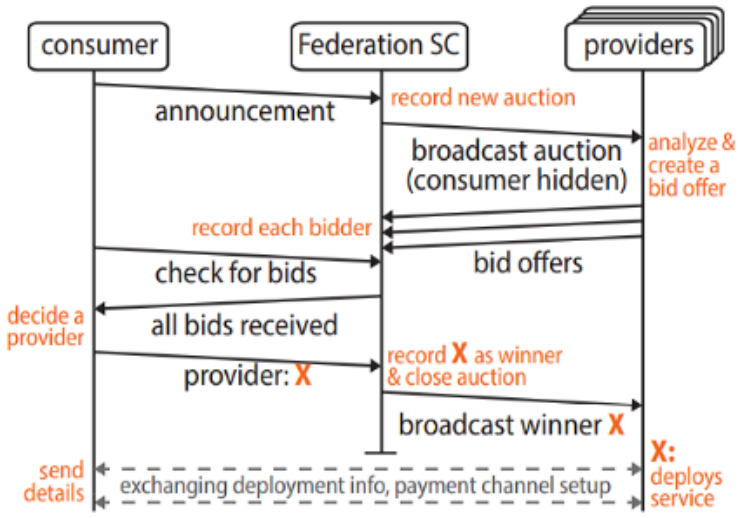


*Figure 2: Sequence of communications as part of the federation process [1].*

A. Technologies with 5G Federation

With technology evolving, research is being conducted to find ways to incorporate innovative technologies with 5G to improve performance and security. Blockchain and Machine Learning (ML) are emerging technologies researchers are looking to integrate into the federation process. These technologies provide solutions to federation problems and introduce new features, which will help improve the future of 5G services and resources.

Blockchain, as [10] puts it, is a digital ledger technology (DLT) that contains a history of transactions and events in a database. Once information is stored in a blockchain, it cannot be erased. Blockchain can be used in the federation process for security and transparency between service providers. For example, once a customer accepts an offer from a service provider after the bidding process, payment information will be kept confidential with blockchain encrypting messages.

Machine Learning (ML) is a part of artificial intelligence (AI) where systems consume information to learn and improve with any instructions [14]. ML requires an algorithm to analyze different data and learn over time. After it learns enough information through the data provided, it can be used to make predictions and decisions automatically for 5G. For example, ML could allow for better resource management, as it learns when resources need to be used more often or not

used. The following section will discuss recent literature covering key technologies that are helping advance the federation of 5G services and resources.

## III. Literature Review

### A. Federation With Blockchain

Blockchain is the use of cryptography to store data in secure blocks, which contain linked records of transactions. Some of blockchain's features that can be used in the federation process include transparency, automation, and increased security. Using distributed ledgers with a permissioned blockchain, all participants in the network will have the same information on transactions and data. This eliminates potential fraudulent transactions during the federation process. With smart contracts, communications between ADs are triggered automatically once conditions are met. This increases process efficiency and reduces the need for human intervention. Blockchain also has properties, such as linking transaction information together over time, which makes it difficult to manipulate any information within the blocks. Once information is entered into the blockchain, it cannot be modified.

Many proposals have been made that use blockchain to improve the federation process for 5G services and resources. [1] proposed applying distributed ledgers for distributed interactions over multiple administrative domains. This proposal improves security, privacy, and efficiency when administrative domains interact during the federation process. It also requires a one-time setup with fast registration times for the administrative domains. The conducted experiments reveal that the mining time in this process remained about the same with any number of transactions and that the total federation time remained linear as more bidders were involved. [2] discusses using blockchain by implementing smart contracts as a network slice (NS) broker. The smart contracts will be used for automating the negotiations/agreements related to slice-brokering functions. This improves the effectiveness of negotiations for Service Level Agreements (SLA) and reduces the complexity of coordinating these communications. [3] proposed using a distributed broker system with a blockchain-based bidding system for requesting and distributing resources over various domains securely. This process is designed for network operators to communicate these requests with each other in a transparent manner. This provides effective resource provisioning, security, and high-speed performance for federating services and resources.

With blockchain's valuable features, some issues could impact resource and service federation. A review of applications of blockchain in 5G [16] expressed concerns with large amounts of bandwidth being consumed, resulting in overhead. To reach a consensus during the federation process, blockchain requires a lot of bandwidth and power. When blockchain broadcasts transactions to be approved during the blockchain process, it results in considerable overhead added to the network traffic that could impact network bandwidth. Not only will this impact bandwidth, but reaching a consensus could take longer with the imposed resource constraints. [15] and [16] both discuss another issue, which is scalability with blockchain. Blockchain can only handle a certain number of Transactions Per Second (TPS) and store a certain amount of data before performance is affected. 5G's goal is to provide high throughput communication, and the

federation process should be quick and efficient, from request to service deployment. If blockchain cannot handle an increase in transactions and storage, it will impact the user's experience.

Blockchain is also susceptible to various types of attacks that could impact resource and service federation. [18] describes different blockchain attacks, such as Man-In-The-Middle (MITM) and malleability attacks, that could negatively impact the federation process. A man-in-the-middle attack can be used to target device or service provider information being shared using blockchain. This type of attack violates user privacy and is used to gather/alter sensitive data. If a malicious actor coordinates this attack, they can intercept the conversation between ADs and/or service providers, collect user information, and alter these conversations. Tampering with the information sent in this process could change the outcome of the federated service and/or resources, leading to potential financial, legal, and resource allocation issues. A malleability attack is the ability to change a transaction's digital signature before it's assigned to the chain, without invalidating it. Because this attack is performed before the transaction is validated, it is viewed as a valid transaction and is then validated. During the federation process, having a validated transaction, which is a fake transaction, could affect the outcome of the federated service and/or resources.

Table 1 provides an overview of the discussed proposals for utilizing blockchain technology to enhance the federation of 5G services and resources. The reference section of the table provides index numbers for the studies and detailed proposals for further reading.

*Table 1: Federation Examples Utilizing Blockchain.*

| Ref. | Use Case | How It's Used | Problem Solved | Challenges |
|---|---|---|---|---|
| [1] | Use distributed ledger technologies for the federation of 5G services and interactions between administrative domains | Where each administrative domain runs a single node in the network, a permissioned blockchain is implemented. A Federation Smart Contract (FSC) is installed on the blockchain to run as a distributed authority. | - Smart contracts add security and trust among participants<br>- Simple one-time system set up with fast registration time<br>- Service federation is executed quickly, no matter the number of bidding provider domains<br>- Improves interaction between administrative domains that federate network services | - Potential high maintenance costs |
| [2] | Multi-operator network slicing with blockchain | Deploying smart contracts and blockchain as a distributed ledger in a network slice broker system. The network slice broker handles the allocation of resources and network traffic supervision. | - Transactions are verified with signatures and time stamps to prevent non-repudiation problems<br>- Smart contracts help reduce coordination complexity<br>- Reduces transaction costs | - Requires a large amount of data storage<br>- Power consumption |
| [3] | Resource provisioning using a distributed blockchain-based broker | A blockchain-based bidding system is used for network operators to provide and request resources. These requests are secure, transparent, and quick. | - Removes the need for the long memorandum of understanding (MoU) process<br>- Allows for Service Level Agreement (SLA) requirements from network operators through monitoring of cross-domain resource Quality of Service (QoS) metrics<br>- Improved throughput (comparing DBB (Distributed Brokering System) video traffic with non-DBB video traffic) | - Needs more types of network traffic to compare with |

### B. Federation With Machine Learning

Machine Learning (ML), as described in [6], is the ability of a computing system to learn by extracting data without any instructions. This is done using algorithms to analyze various kinds of data. Some of ML's features used in the federation process include predictive modeling, automation, and adaptiveness [8]. Predictive modeling can be used in the federation process to determine when to expect certain events. For example, it can predict the number of resource requests per day or determine when there is the potential for service and/or resource failure. ML can use the data it learns to start automating tasks, such as enabling and disabling features, which reduces the need for human intervention. ML can also adapt to new data, as algorithms were designed to continuously learn. This data could be related to new services, resources, and/or current mobile network trends, which allows for improved performance and precision as more information becomes available.

Many proposals use ML to improve the federation process for 5G services and resources. [11] proposed using times series forecasting analytics, a ML technique, with 5G Core network data to predict events and improve network performance. By collecting information on resource usage, such as the rate of operation failures over time, the ML algorithm can predict the workload on the network, improve resource management, and use the data to avoid unforeseen failures. [12] introduces a Q-learning algorithm that produces decisions for increasing revenue without additional processing and computation for resources. This solution benefits ADs by making profitable decisions and increasing efficiency during the federation process. The Q-learning algorithm was tested to show its effectiveness in different scenarios, such as deploying resources quickly with or without checking available resources and calculating potential profit based on these scenarios. [13] introduced an orchestration methodology for session-based services using deep reinforcement learning. A ML algorithm is used to help make decisions on federating online session-based services, such as video games and video conferences. The framework's goal is to maximize the QoS and minimize the number of resources needed to be federated while providing reliable and consistent services for users.

Despite ML's valuable features, some issues could impact resource and service federation. [5] discusses concerns about ML misconfigurations. When ML algorithms begin to learn what to do using the data provided, there is a chance for errors and incorrect configurations to occur. When federating resources and/or services, these misconfigurations could impact performance, security, and availability. With more data becoming available over time and the algorithm continuing to learn, misconfigurations are less likely to occur. [7] discusses the concern of fake datasets being uploaded for ML training. Fake datasets are used to train ML to do incorrect things or to replace all real data with unsolicited data. This can result in misconfiguration, with similar impacts on performance and security. It could also impact predictive modeling and automation used for federation.

ML is also susceptible to various types of attacks that could impact resource and service federation. [19] describes different ML attacks, such as data and model poisoning attacks, that could affect the federation process. A data poisoning attack is when ML training data is tampered

with, leading to the algorithm producing unexpected outputs. This impacts the performance of the algorithm and decreases its accuracy when making important decisions. If the tampered data is not detected early in the learning process, restarting this process from the beginning will take a long time, which is not ideal for users. Tampering with ML training data will also impact decision-making in the federation process. For example, when determining the best option when requesting services and/or resources, the ML algorithm will most likely not pick the option based on what it knows. A model poisoning attack is used to influence the machine learning algorithm. This attack focuses on changing the algorithm and does not tamper with the data already used. By tampering with the model and algorithm, future data that is used as input may lead to issues like miscategorized data and the potential for backdoors to be inserted into the model.

Table 2 provides an overview of the discussed proposals for utilizing ML technology to improve the federation of 5G services and resources. The reference section of the table provides index numbers for the studies and detailed proposals for further reading.

*Table 2: Federation Examples Using Machine Learning.*

| Ref. | Use Case | How It's Used | Problem Solved | Challenges |
|---|---|---|---|---|
| [11] | Time Series Forecasting in Software 5G Networks | - Time series forecasting (an essential field of Machine Learning) is used with 5G core to predict future network events and potential resource usage.<br>- Predictions can be used to determine whether accepting resource requests will impact resource usage and availability.<br>- Uses a supervised learning algorithm. | - Improved resource management<br>- Can predict unexpected failures to occur within the 5G network<br>- Automated network management and maintenance | - There is a need for more accurate datasets<br>- Takes time to make more accurate decisions |
| [12] | Resource federation algorithm that makes decisions for Administrative Domains (ADs) | - A Q-learning algorithm (value-based) is used to make federation deployment decisions that provide a revenue increase and improved computational efficiency.<br>- Uses a reinforcement learning algorithm. | - Resource management to prevent resource shortage<br>- No increase in re-calculations and processing for available resources and services | - The state space grows with more federation components to represent |
| [13] | Service orchestration for session-based services based on a deep reinforcement learning framework | - A ML service orchestration algorithm is used to make decisions to provide high-quality performance for session-based applications/services.<br>- Uses a reinforcement learning algorithm. | - Saving resources by making decisions to minimize the amount needed<br>- Improved QoS | - There is a need for improvements in effective resource management<br>- Some specific deployment requirements may affect the network performance |

## IV. Discussion and Future Directions

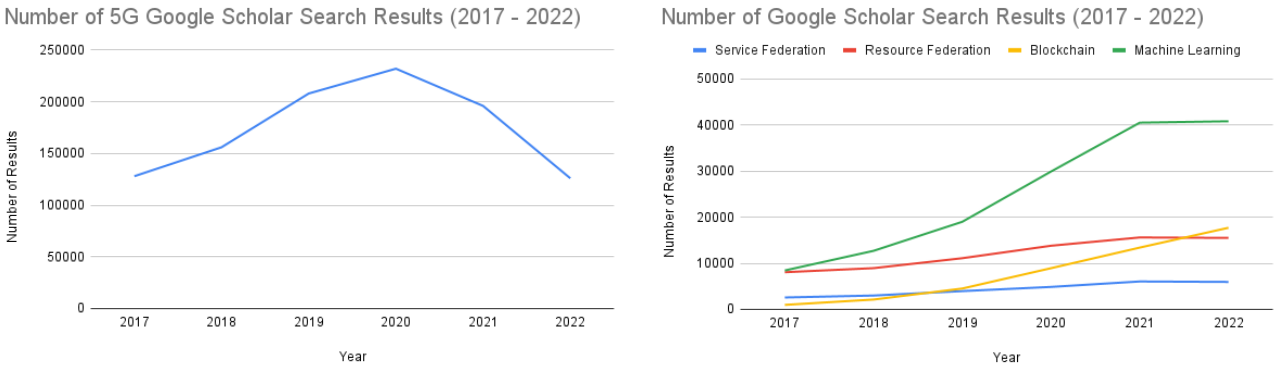


*Figure 3: Google Scholar search results on 5G and federation technologies within the last 5 years.*

Recent research outcomes have provided insight into how 5G federation can become more advanced with blockchain and ML. The federation process can further expand with these technologies to address the concerns of resource management, privacy, and Quality of Service (QoS). Blockchain provides secure communication, transparency, and smart contracting for the federation process to address privacy issues. ML provides automation and data analysis for better management and improved quality of federated resources and/or services. Over the last few years, 5G has grown from an idea into a reality. Not only is 5G used in smartphones, but it is expanding its capabilities by being used in cars, Internet of Things (IoT) devices, and more in the future. Furthermore, 5G networks will continue utilizing a variety of technologies to make it the best it can be. Figure 3 shows the number of Google Scholar papers on 5G, resource and service federation, and the discussed technologies for improving the federation process. Research on these topics, such as ML, appears to be increasing over time. This is due to further developments in a variety of ML topics, such as Artificial Intelligence, reinforcement learning, and deep learning.

### A. Blockchain

Looking back at Table 1 in Section III, each example used blockchain with 5G federation in different ways. [1] used distributed ledger technology to help improve the process of federating 5G services across multiple domains. Although the experiments show the solution is effective at completing AD registration quickly in the federation process, there are other variables, like client and node machine hardware and operating system, that could be changed to see if it alters performance. [2] utilized smart contracts in a network slice broker system for higher transparency and transaction validation in the federation process. The paper provides a detailed description of the allocation procedure, with a diagram representing the proposal, but does not experiment with their proposed solution. Testing the proposal would improve the credibility of the work and could provide researchers with information to experiment further. [3] uses a distributed blockchain-based broker that creates a bidding system with blockchain for providing and requesting resources. An experiment comparing video streaming quality with and without the proposed system revealed that streaming quality was improved with the system. While this experiment provided us with

information on video quality, the paper lacks testing on other performance metrics, such as download speed, upload speed, and game performance.

Based on the recent discussions on blockchain within the federation process, certain aspects could be researched further. One future research direction is scalability. Due to slow transaction speeds with certain blockchain implementations, it may be challenging to use in the 5G federation process. Service and resource federation was designed to be quick and straightforward for both customers and providers, but blockchain could alter this process. Although [2] discusses how blockchain with 5G helps increase network performance and scalability, the majority of recent work discusses challenges with scalability with blockchain Finding ways to improve transaction speeds without affecting federation performance should be studied further. Another future research direction is storage management. Depending on the number of services and resources ADs can provide, the amount of data stored in a blockchain always increases, as the data is never altered or removed. When receiving requests for resources from other ADs, it is important to consider how much data will need to be stored in a blockchain in the future. [15] discusses how further research is needed to find ways to condense or better manage data stored in a blockchain, along with improved blockchain architectures and consensus algorithms. This would allow for more resource requests without the need to buy more storage. One final future research direction is data handling. Finding a way to determine what parts of the federation process could use blockchain and what information wouldn't need its features. It would be ideal to use blockchain only for specific steps or components that need improvement, preventing significant impacts on performance. Finding ways to determine higher priority data in the 5G federation process that should use blockchain, potentially using ML for decision-making, is something that should be studied. [15] discusses choosing high-priority parameters to store in its blockchain, such as start and termination times for service, QoS parameters, and charging evidence, due to expensive data storage costs. Table 3 provides an overview of topics related to blockchain that could be researched further to improve federation.

*Table 3: Summary of Future Opportunities with Blockchain.*

| Research Direction | Challenges | Considerations |
|---|---|---|
| **Scalability** | - Slow transactions<br>- Limits on the number of transactions (depending on the type of blockchain)<br>- Lengthy transaction times can affect performance | - Methods of increasing transaction speeds without affecting the level of security |
| **Storage Management** | - The amount of data stored in blockchain always increases | - Methods of compressing data stored in blockchain<br>- Methods of splitting up storage to reduce the storage usage on a single node |
| **Data Handling** | - Determining where in the federation process blockchain would be most beneficial<br>- Determining what data should be stored in a blockchain | - Every step in the federation process doesn't need to use blockchain<br>- Experiments on different steps in the federation process to identify where blockchain could work and where it could cause potential complications |

## B. Machine Learning

Looking back at Table 2 in Section III, each example used ML with 5G federation in different ways. [11] used a subsection of ML, time series forecasting, and the 5G core model to help predict future network and device events using resource usage statistics in the federation process. Although few datasets are available, the experiment conducted demonstrates the solution's ability to predict memory and CPU usage over time. If future experiments are conducted based on this solution, other performance metrics, such as the amount of data traffic and component temperatures, can be evaluated for future component predictions. [12] proposes a value-based reinforcement learning algorithm for service and resource deployment decisions that are most profitable and optimal. Experiments on the learning rate, discount factor, and performance of the Q-learning algorithm reveal favorable results in overall performance compared to other federation approaches. The authors of the paper focus on the importance of profiting from deployment decisions, but future papers can expand on other advantages of algorithm decision-making for both customers and providers, such as automation, downtime prevention, resource, and scalability decisions. [13] focuses on the federation of session-based services using a deep reinforcement learning algorithm to make service orchestration decisions to improve performance. When assessing this solution, experiment results displayed its ability to handle high-load scenarios, use a small number of resources, and exhibit computation times that are suitable for real-time processes. The authors of this paper provided information on many experiments completed and suggested further research on other algorithms and edge computing models.

Based on the recent discussions on ML within the federation process, certain aspects could be researched further. One future research direction is evaluating how network topologies could affect ML framework performance. The way a network is organized and designed can potentially affect how a ML algorithm runs, but determining what factors could impact the framework's performance is something to be studied. Device configurations, device types, network connections, and enabled features are factors that may influence performance and should be assessed. Another future research direction is energy consumption. Like blockchain, ML requires a lot of computational power and storage. The training phase is the most essential part of the ML process, which uses the most power and resources. Because the training process is important for assuring the efficiency and effectiveness of the algorithm in the future, it is difficult to find ways to use less power or energy. A few practical solutions exist to reduce the load on storage and resources, like deploying ML on the cloud, but that could create other issues like data mobility and the risk of information exposure to public networks. Finding alternative methods of reducing energy consumption without any detrimental impacts can be further researched. The final future research direction is the lack of datasets. There are some datasets available online for ML efforts, but even fewer for 5G and service federation. We need more diverse datasets focused on security, prediction models, and resource management to further 5G federation research developments. Finding ways to create more datasets for public use or collaborating with companies affiliated with mobile networks to get data for testing are suggestions to consider. [6] discusses how researchers have

limited access to datasets and how telecommunication companies are not willing to share this information. It also mentions that researchers are attempting to create their own datasets with limited information available to the public. Table 4 provides an overview of topics related to ML that could be researched further to improve federation.

*Table 4: Summary of Future Opportunities with Machine Learning.*

| Research Direction | Challenges | Considerations |
|---|---|---|
| **Network Topologies Impacting ML Performance** | - Variables like device type, configurations, and network communications could affect the performance of a ML algorithm | - Conduct experiments on various ML algorithms and change different variables to see if there are any changes in performance |
| **Energy Consumption** | - A lot of power and energy is required for the ML training phase<br>- Power and energy management is important for all services and resources and should be distributed fairly | - Methods of transferring a part or all ML resources to a cloud service or off-site provider, without impacting its configurations and running processes. |
| **Lack of Datasets** | - There are almost no datasets available related to federating 5G services and resources<br>- More datasets need to be created by researchers and/or companies for public use | - Collaborations with mobile service providers to get any type of dataset available for public use or providing datasets to private researchers to share experiment results<br>- Find ways to get real-world data |

## A. Open AI Cellular (OAIC)

Open AI Cellular (OAIC) is an open-source effort that provides libraries and toolsets that contain AI controllers and an AI testing framework [20]. This effort helps towards development and research on AI-enabled cellular radio networks. OAIC provides a framework, as shown in Figure 4, that acknowledges various open-source 5G software, which allows users to implement radio access network intelligent controllers (RICs) and O-RAN interfaces for testbed and production real-time experiments.

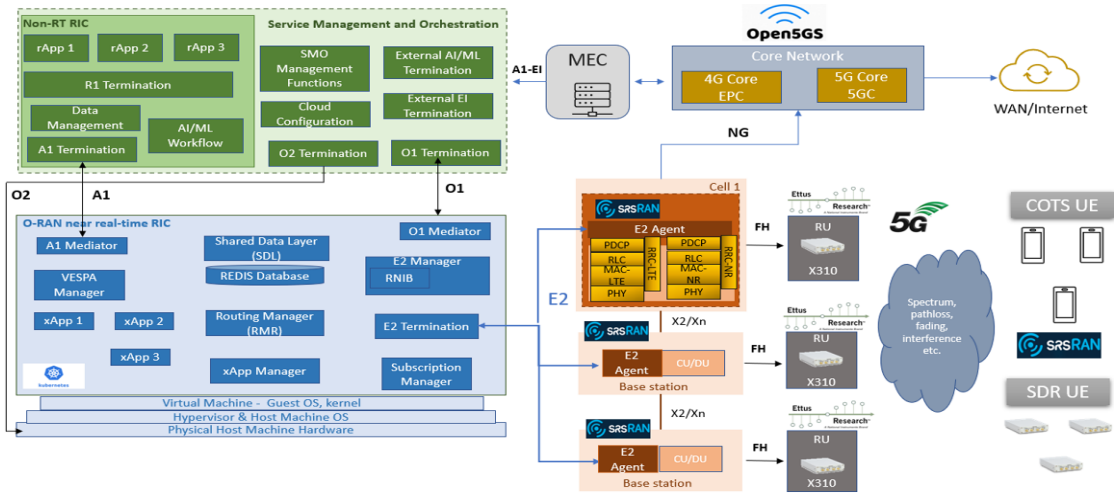


*Figure 4: Open AI Cellular (OAIC) Framework [20].*

OAIC provides instructions for allowing users to create their own 5G network. This can be used for testing 5G network components, learning about 5G, and developing tools and software related to mobile networks. When running a 5G network with OAIC, there are a few components used that are important to know. The first component is the EPC, which represents the core of the network. It is used for session management, mobility management, and authentication. The second component is the gNB/gNodeB, which functions like a base station, providing connectivity between the EPC and the user. The third component is the User Equipment (UE), which is the mobile device that will be connected to the 5G network. Figure [NUMBER] shows each of the components in separate terminal windows.

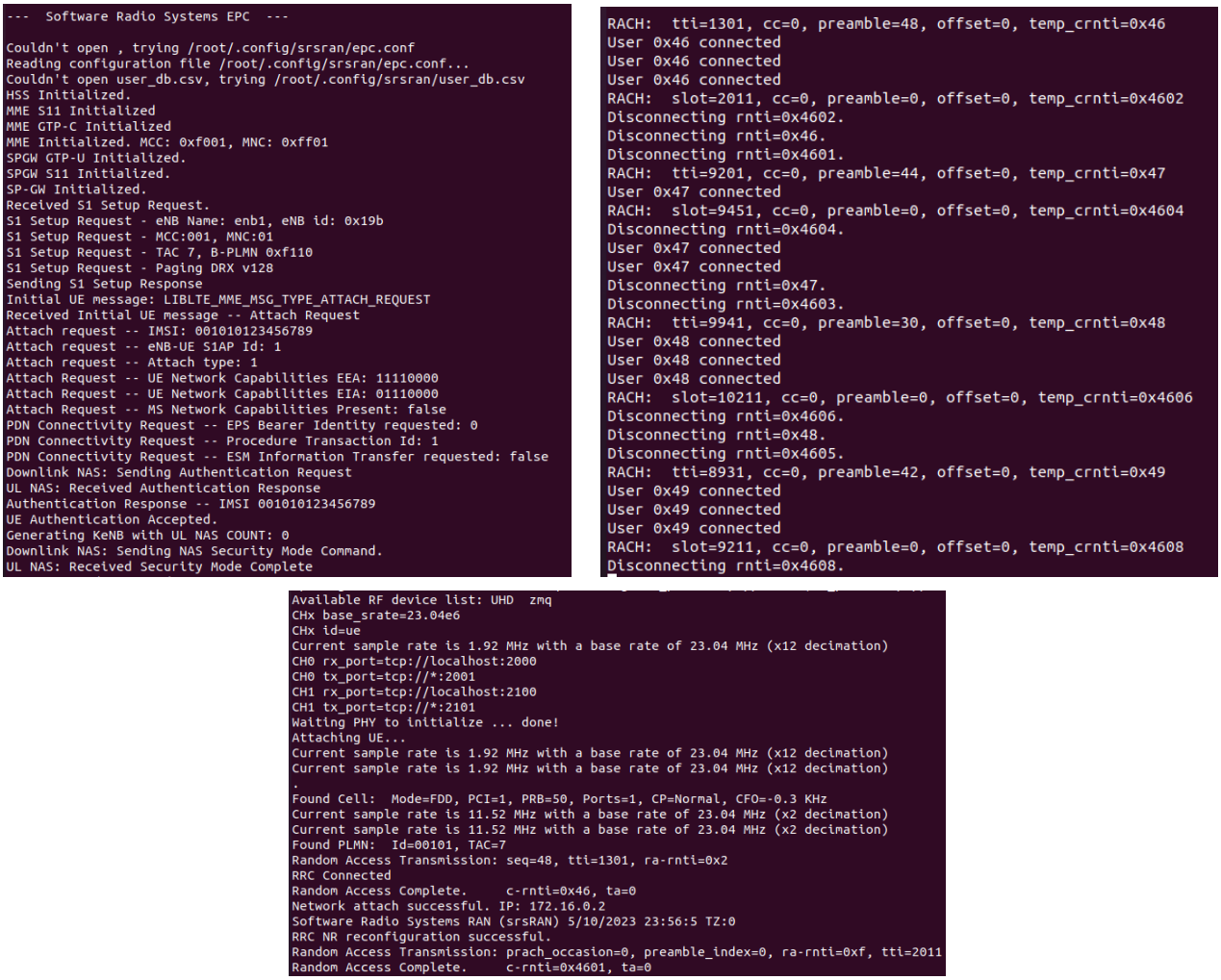


*Figure 5: The top left terminal represents the EPC. The top right terminal represents the gNodeB. The bottom terminal represents the UE.*

## V. Practical Experiments and Results

Our first experiment will test how well components within the configured OAIC installation can handle Denial-of-service (DOS) traffic. We ran normal traffic (pings) on the simulated 5G network for 2 hours to get a baseline of data rates, amount of traffic sent, and component

performance. After running normal traffic, we ran a DOS attack on the gNodeB for 2 hours to compare component performance with the normal traffic performance.

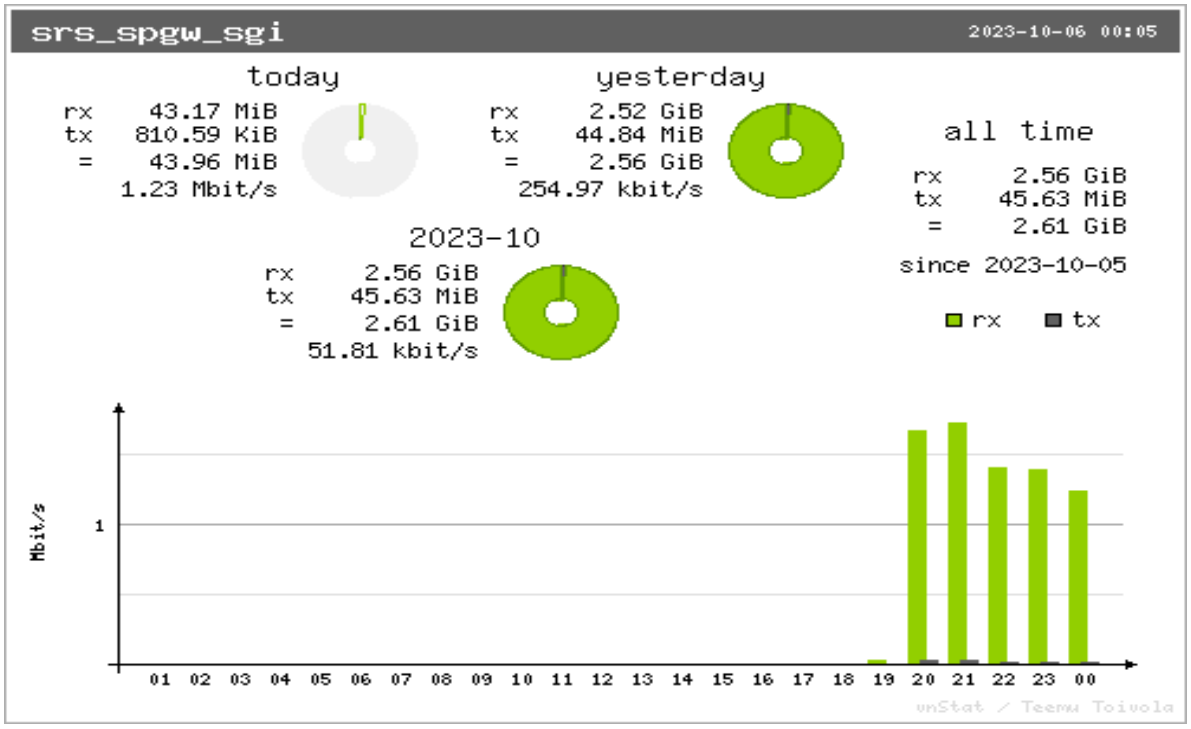


*Figure 6: The bit rate of the 5G network per hour. Hours 20 and 21 are with normal traffic, and hours 22 and 23 are with DOS attack traffic.*

For the normal traffic, we used vnStat [21] to track network and component performance and ping to send traffic within the network. This will be used as a baseline to see how the network performance is without any large traffic. We would ping for 2 hours, then transition into running a DOS attack on the gNodeB. We used hping3 to flood the network with requests for our DOS attack to see how it would impact overall performance. While monitoring normal and DOS traffic, we used vnStat to create a graph showing data rates per hour, logged ping time to see if there were any delays in responses, and logged iperf [22] bitrates from the user equipment and network side. The results from this experiment show that there is a noticeable decrease in bit rate and longer response times while running the DOS attack. Figure 6 shows the bit rate from the network interface srs_spgw_sgi, which is where this AI-enabled 5G network is running. The figure shows the bit rate increasing from hour 20 to 21, which is when the normal traffic was sent. It also shows that from hour 21 to 00, the bit rate was decreasing, which was when the DOS attack was running.

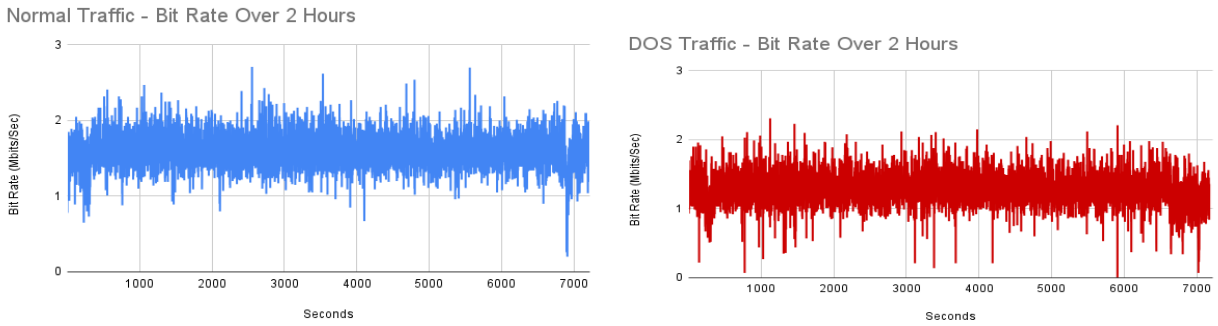


*Figure 7: A comparison of bit rates during normal traffic and DOS traffic.*

Figure 7 shows the second-by-second bit rate of the base station, tracked with iperf, from both the normal and DOS traffic over 2 hours. The normal traffic bit rate is higher overall, while the DOS traffic is lower and has multiple spikes where the bit rate drops close to 0.

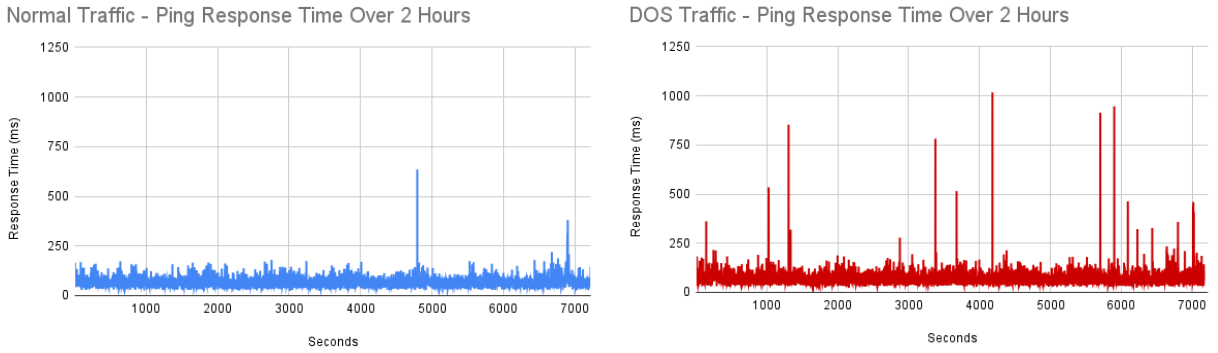


*Figure 8: A comparison of ping response time during normal traffic and DOS traffic.*

Figure 8 shows the second-by-second ping response time when pinging the base station during normal and DOS traffic over 2 hours. The response time was quicker during normal traffic, while there were moments during the DOS traffic when it would take more than 500ms for a response. The attack appears to have impacted the network response time, with many spikes in response time.

```
root@andrew-VirtualBox:~/oaic/nexran# curl -i -X PUT -H "Content-type: application/json" -d '
{"allocation_policy":{"type":"proportional","share":1024}}' http://${NEXRAN_XAPP}:8000/v1/sli
ces/slow ; echo ; echo
HTTP/1.1 200 OK
Connection: Close
Content-Length: 0
```

```
root@andrew-VirtualBox:~/oaic/nexran# curl -i -X PUT -H "Content-type: application/json" -d '
{"allocation_policy":{"type":"proportional","share":256}}' http://${NEXRAN_XAPP}:8000/v1/slic
es/fast ; echo ; echo
HTTP/1.1 200 OK
Connection: Close
Content-Length: 0
```

*Figure 9: Implementing slow slicing (top) and fast slicing (bottom).*

Our second experiment will test how well components within the configured OAIC installation with RAN slicing can handle Denial-of-service (DOS) traffic. OAIC offers two different ways of implementing RAN slicing, which includes slow and fast slices. Slow slicing is where there are fewer slices, meaning higher data rates for each slice. Fast slicing is where there are more slices, meaning lower data rates. For each type of slicing, we collected ping and iperf information in normal traffic for 2 hours, then collected the same information while under a DOS attack for 2 hours. Figure 9 shows the implementation of slow and fast slices on the simulated 5G network.

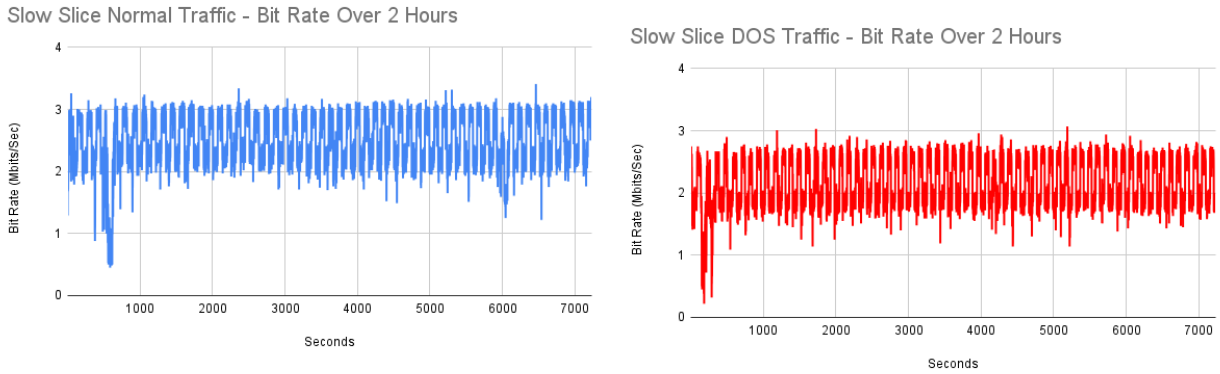


*Figure 10: A comparison of bit rates during slow-sliced normal traffic and DOS traffic.*

For the slow slices, the results from this experiment show that there is a noticeable decrease in bit rate and slightly longer response times. Figure 10 shows the second-by-second bit rate of the base station with slow slices, tracked with iperf, from both the normal and DOS traffic over 2 hours. The normal traffic bit rate is higher overall, while the DOS traffic is lower, and both had a large spike towards the beginning where their bit rate reached below 1 Mbit/sec. When comparing these results to the non-sliced network, the slow sliced network had jumps in data rates from high to low, which is something to pay attention to. There are also fewer spikes where the bit rate reaches below 1 Mbit/sec.

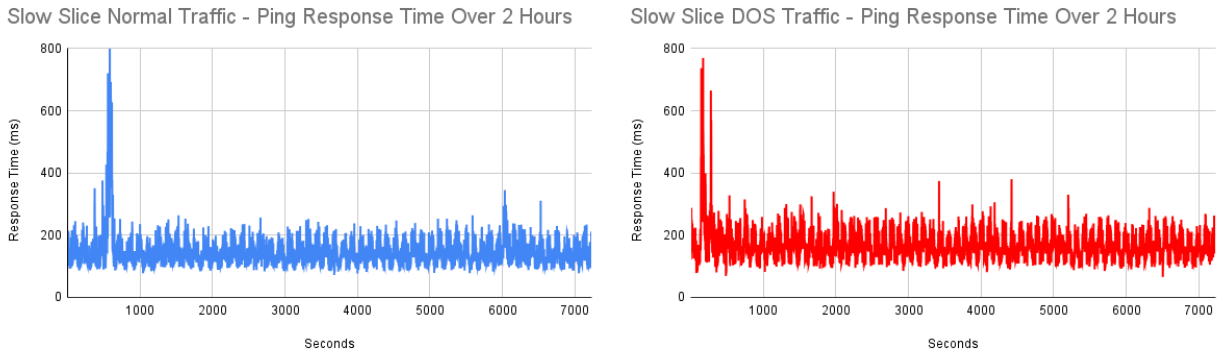


*Figure 11: A comparison of ping response time during slow-sliced normal traffic and DOS traffic.*

Figure 11 shows the second-by-second ping response time when pinging the base station with slow slices during normal and DOS traffic over 2 hours. The ping response time was faster during normal traffic, but there were only a few spikes where the response time was almost 400ms. Compared to the non-sliced network, there were fewer spikes in response time, except for one huge spike in the slow sliced network towards the beginning.

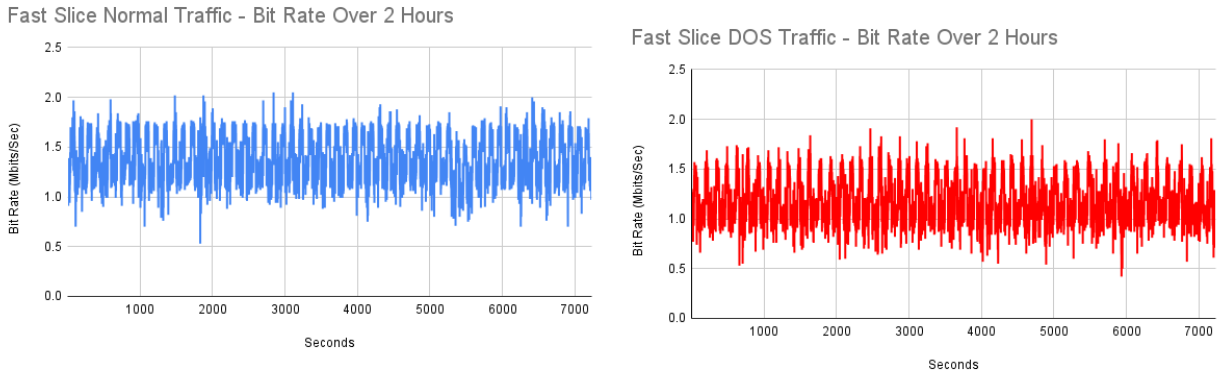


*Figure 12: A comparison of bit rates during fast-sliced normal traffic and DOS traffic.*

For the fast slices, the results from this experiment show that there is a slight decrease in bitrate during a DOS attack. Figure 12 shows the second-by-second bit rate of the base station with fast slices, tracked with iperf, from both the normal and DOS traffic over 2 hours. Although the bit rate during the DOS is slightly lower, it appears the attack did not have a large impact. The fast slices were able to manage this attack very well.

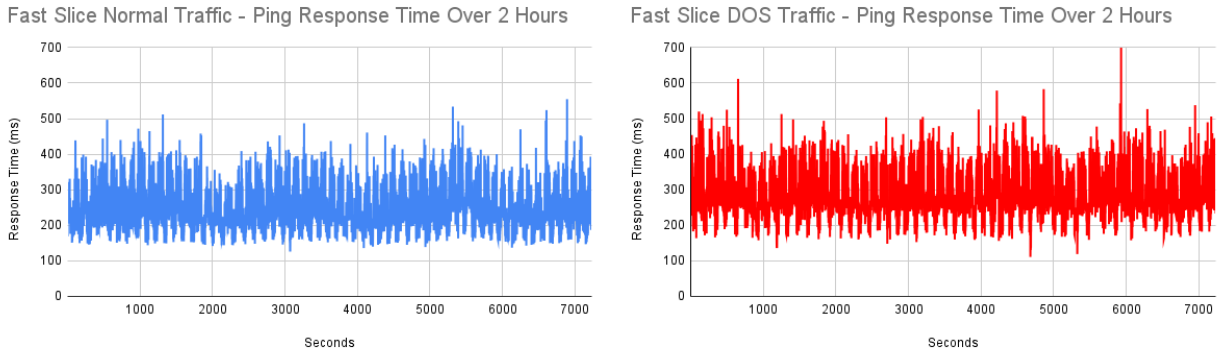


*Figure 13: A comparison of ping response time during fast-sliced normal traffic and DOS traffic*

Figure 13 shows the second-by-second ping response time when pinging the base station with fast slices during normal and DOS traffic over 2 hours. There is a noticeable difference in response time between the normal and DOS traffic. The DOS traffic had longer response times compared to normal traffic, which is the common trend with each of these experiments. Compared to the slow slices, the response time had a wider range of response times. The fast slices ping response time averaged between 150 to 500ms, while the slow slices averaged between 200 and 300ms.

Based on the results of these experiments, the RAN-sliced 5G network appeared to handle the DOS attack better than the regular 5G network. The RAN sliced network had little to no drops in bit rate and fewer large spikes in ping response time compared to the regular network. This experiment reveals that a DOS attack can impact the AI-enabled mobile network's performance, but implementing RAN slicing could reduce the effects on network performance. For future experiments, longer tests could be conducted, along with testing other types of network attacks on the simulated 5G network.

## VI. Conclusion

5G continues to evolve as emerging technologies are implemented to meet users' performance, security, and privacy needs. This paper has provided insight into what federating services and resources can do for the future of 5G. Our literature review describes various approaches for using blockchain and ML to expand the capabilities of federating 5G resources. The review also highlights the advantages, disadvantages, and challenges associated with 5G federation and other technologies, i.e., blockchain and ML. We experimented with an AI-enabled 5G network to learn more about AI in mobile networks and to see how different factors affect network performance. Finally, we share our analysis of what recent literature could've done, along with future directions and limitations for future research. For future work, we plan to extend the current work with the cybersecurity and 5G work listed in [23-97] to implement the proposed technologies.

## VII. References


[1] Antevski, K, Bernardos, CJ. Federation of 5G services using distributed ledger technologies†. Internet Technology Letters. 2020; 3:e193. https://doi.org/10.1002/itl2.193

[2] G. Praveen, V. Chamola, V. Hassija and N. Kumar, "Blockchain for 5G: A Prelude to Future Telecommunication," in IEEE Network, vol. 34, no. 6, pp. 106-113, November/December 2020, doi: 10.1109/MNET.001.2000005.

[3] Togou, M. A., Bi, T., Dev, K., McDonnell, K., Milenovic, A., Tewari, H., & Muntean, G.-M. (2020). A Distributed Blockchain-based Broker for Efficient Resource Provisioning in 5G Networks. 2020 International Wireless Communications and Mobile Computing (IWCMC). doi:10.1109/ iwcmc48107.2020.9148565

[4] Qualcomm. "Everything you need to know about 5G.," [Online]. Available: https://www.qualcomm.com/5g/what-is-5g.

[5] Suomalainen, J., Juhola, A., Shahabuddin, S., Mammela, A., & Ahmad, I. (2020). Machine Learning Threatens 5G Security. IEEE Access, 8, 190822–190842. doi:10.1109/access.2020.3031966

[6] M. E. Morocho-Cayamcela, H. Lee and W. Lim, "Machine Learning for 5G/B5G Mobile and Wireless Communications: Potential, Limitations, and Future Directions," in IEEE Access, vol. 7, pp. 137184-137206, 2019, doi: 10.1109/ACCESS.2019.2942390.

[7] Afaq, A., Haider, N., Baig, M. Z., Khan, K. S., Imran, M., & Razzak, I. (2021). Machine learning for 5G security: Architecture, recent advances, and challenges. Ad Hoc Networks, 123, 102667. doi:10.1016/j.adhoc.2021.102667

[8] Cointelegraph. "5 key features of machine learning.," [Online]. Available: https://cointelegraph.com/news/5-key-features-of-machine-learning.

[9] Baran, Paul, On Distributed Communications: I. Introduction to Distributed Communications Networks. Santa Monica, CA: RAND Corporation, 1964. https://www.rand.org/pubs/research_memoranda/RM3420.html.

[10] M. Crosby et al., BlockChain Technology Beyond Bitcoin, Oct. 2015, [online] Available: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.

[11] Chakraborty, P., Corici, M., & Magedanz, T. (2020). A comparative study for Time Series Forecasting within software 5G networks. 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS). doi:10.1109/icspcs50536.2020.9310033

[12] Antevski, K., Martin-Perez, J., Garcia-Saavedra, A., Bernardos, C. J., Li, X., Baranda, J., … Vettori, L. (2020). A Q-learning strategy for federation of 5G services. ICC 2020 - 2020 IEEE International Conference on Communications (ICC). doi:10.1109/icc40277.2020.9149082

[13] Chen, Wen & Chen, Yuhu & Wu, Jiaxing & Tang, Zhangbin. (2021). A multi-user service migration scheme based on deep reinforcement learning and SDN in mobile edge computing. Physical Communication. 47. 101397. 10.1016/j.phycom.2021.101397.

[14] Oracle. "What is Machine Learning?.," [Online]. Available: https://www.oracle.com/artificial-intelligence/machine-learning/what-is-machine-learning.

[15] Chaer, A., Salah, K., Lima, C., Ray, P. P., & Sheltami, T. (2019). Blockchain for 5G: Opportunities and Challenges. 2019 IEEE Globecom Workshops (GC Wkshps). doi:10.1109/gcwkshps45667.2019.9024627

[16] M. Tahir, M. H. Habaebi, M. Dabbagh, A. Mughees, A. Ahad and K. I. Ahmed, "A Review on Application of Blockchain in 5G and Beyond Networks: Taxonomy, Field-Trials, Challenges and Opportunities," in IEEE Access, vol. 8, pp. 115876-115904, 2020, doi: 10.1109/ACCESS.2020.3003020.

[17] Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjoland, H., & Tufvesson, F. (2021). 6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities. Proceedings of the IEEE, 109(7), 1166–1199. doi:10.1109/jproc.2021.3061701

[18] Sabreen Ahmadjee, Carlos Mera-Gómez, Rami Bahsoon, and Rick Kazman. 2022. A Study on Blockchain Architecture Design Decisions and Their Security Attacks and Threats. ACM Trans. Softw. Eng. Methodol. 31, 2, Article 36e (April 2022), 45 pages. https://doi.org/10.1145/3502740

[19] Sikandar HS, Waheed H, Tahir S, Malik SUR, Rafique W. A Detailed Survey on Federated Learning Attacks and Defenses. Electronics. 2023; 12(2):260. https://doi.org/10.3390/electronics12020260

[20] Open ai cellular (OAIC). Open AI Cellular (OAIC). (n.d.). https://www.openaicellular.org/

[21] VnStat - a network traffic monitor for linux and BSD. (n.d.). https://humdi.net/vnstat/

[22] Iperf - the ultimate speed test tool for TCP, UDP and SCTPTEST the limits of your network + internet neutrality test. iPerf.fr. (n.d.). https://iperf.fr/

[23] A. A. Khalil, M. A. Rahman and H. A. Kholidy, "FAKEY: Fake Hashed Key Attack on Payment Channel Networks," 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2023, pp. 1-9, doi: 10.1109/CNS59707.2023.10288911.

[24] Hisham A. Kholidy, Fabrizio Baiardi, A. Azab, "A Data-Driven Semi-Global Alignment Technique for Masquerade Detection in Stand-Alone and Cloud Computing Systems", is Submitted in ", granted on January 2019, US 20170019419 A1.

[25] Hisham A. Kholidy, "Accelerating Stream Cipher Operations using Single and Grid Systems", US Patent and Trademark Office (USPTO), April 2012, US 20120089829 A1.

[26] Hisham Kholidy, "Multi-Layer Attack Graph Analysis in the 5G Edge Network Using a Dynamic Hexagonal Fuzzy Method", Sensors 2022, 22, 9. https://doi.org/10.3390/s22010009. (IF: 3.576).

[27] Hisham Kholidy, "Detecting impersonation attacks in cloud computing environments using a centric user profiling approach", Future Generation Computer Systems, Volume 117, issue 17, Pages 299-320, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.009, (IF: 7.307). April 2021, https://www.sciencedirect.com/science/article/pii/S0167739X20330715

[28] Hisham Kholidy, "Autonomous Mitigation of Cyber Risks in Cyber-Physical Systems", Future Generation Computer Systems, Volume 115, February 2021, Pages 171-187, ISSN 0167-739X, (IF: 7.307) DOI: https://doi.org/10.1016/j.future.2020.09.002 https://www.sciencedirect.com/science/article/pii/S0167739X19320680

[29] Hisham A. Kholidy, "An Intelligent Swarm based Prediction Approach for Predicting Cloud Computing User Resource Needs", the Computer Communications Journal, Feb 2020 (IF: 5.047). https://authors.elsevier.com/tracking/article/details.do?aid=6085&jid=COMCOM&surname=Kholidy

[30] Hisham A. Kholidy, "Correlation Based Sequence Alignment Models for Detecting Masquerades in Cloud Computing", IET Information Security Journal, DOI: 10.1049/iet-ifs.2019.0409, Sept. 2019 (IF: 1.51) https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2019.0409

[31] I. Elgarhy, M. M. Badr, M. Mahmoud, M. M. Fouda, M. Alsabaan and Hisham A. Kholidy, "Clustering and Ensemble Based Approach For Securing Electricity Theft Detectors Against Evasion Attacks", in IEEE Access, January 2023, doi: 10.1109/ACCESS.2023.3318111. (IF: 3.55).

[32] Mustafa, F.M., Hisham A. Kholidy, Sayed, A.F. et al. "Backward pumped distributed Raman amplifier: enhanced gain", Optical Quantum Electron 55, 772 (2023). https://doi.org/10.1007/s11082-023-05066-3 (IF: 3.0).

[33] Alahmadi TJ, Rahman AU, Alkahtani HK, Hisham A. Kholidy "Enhancing Object Detection for VIPs Using YOLOv4_Resnet101 and Text-to-Speech Conversion Model", Multimodal Technologies and Interaction. 2023; 7(8):77. https://doi.org/10.3390/mti7080077 (IF: 3.17).

[34] Alkhowaiter, M.; Hisham A. Kholidy.; Alyami, M.A.; Alghamdi, A.; Zou, C, “Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach”. Sensors 2023, 23, 6287. https://doi.org/10.3390/s23146287 (IF: 3.9).

[35] Badr, Mahmoud M., Mohamed I. Ibrahem, Hisham A. Kholidy, Mostafa M. Fouda, and Muhammad Ismail. 2023. "Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems" Energies 16, no. 6: 2852. 2023 (IF: 3.25). https://doi.org/10.3390/en16062852

[36] A Jakaria, M. Rahman, M. Asif, A. Khalil, Hisham Kholidy, M. Anderson, S. Drager, "Trajectory Synthesis for a UAV Swarm Based on Resilient Data Collection Objectives," in IEEE Transactions on Network and Service Management, 2022, doi: 10.1109/TNSM.2022.3216804. (IF: 4.75). https://ieeexplore.ieee.org/document/9928375?source=authoralert

[37] Mustafa, F.M., Hisham Kholidy., Sayed, A.F. et al., “Enhanced dispersion reduction using apodized uniform fiber Bragg grating for optical MTDM transmission systems”. Optical and Quantum Electronics 55, 55 (December 2022). https://doi.org/10.1007/s11082-022-04339-7 . (IF: 2.79).

[38] Hisham A. Kholidy, Abdelkarim Erradi, “VHDRA: A Vertical and Horizontal Dataset Reduction Approach for Cyber-Physical Power-Aware Intrusion Detection Systems”, SECURITY AND COMMUNICATION NETWORKS Journal (IF: 1.968), March 7, 2019. vol. 2019, 15 pages. https://doi.org/10.1155/2019/6816943.

[39] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016. (IF: 2.42).

[40] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, “DDSGA: A Data-Driven Semi- Global Alignment Approach for Detecting Masquerade Attacks”, in IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2014.2327966, May 2014. (ISI Impact factor: 6.791).

[41] Hisham A. Kholidy, Hala Hassan, Amany Sarhan, Abdelkarim Erradi, Sherif Abdelwahed, "QoS Optimization for Cloud Service Composition Based on Economic Model", Book Chapter on the Internet of Things. User-Centric IoT, 2015, Volume 150 ISBN : 978- 3-319-19655-8

[42] Atta-ur Rahman, Maqsood Mahmud, Tahir Iqbal, Hisham Kholidy, Linah Saraireh, et al “Network anomaly detection in 5G networks”, The Mathematical Modelling of Engineering Problems journal, April 2022, Volume 9, Issue 2, Pages 397-404. DOI 10.18280/mmep.090213

[43] Hisham A Kholidy., et al. “A Survey Study For the 5G Emerging Technologies", Acta Scientific Computer Sciences 5.4 (2023): 63-70, DOI: 10.13140/RG.2.2.22308.04485.

[44] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. ElHariri, Ahmed M. Youssouf, and Sahar A. Shehata, “A Hierarchical Cloud Intrusion Detection System: Design and Evaluation”, in International Journal on Cloud Computing: Services and Architecture (IJCCSA), November 2012. DOI 10.5121/ijccsa.2012.2601

[45] Hisham A. Kholidy, Alghathbar Khaled s., “Adapting and accelerating the Stream Cipher Algorithm RC4 using Ultra Gridsec and HIMAN and use it to secure HIMAN Data”, Journal of Information Assurance and Security (JIAS), vol. 4 (2009)/ issue 4,pp 274,tot.pag 283, 2009. http://www.mirlabs.org/jias/vol4-issue6.html

[46] Hisham A. Kholidy, “A Smart Network Slicing Provisioning Framework for 5Gbased IoT Networks”, The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.

[47] Hisham A. Kholidy, “Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis”, IEEE International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, May 1-3, 2019. https://ieeexplore.ieee.org/document/8769482.

[48] Hisham A. Kholidy, "A Study for Access Control Flow Analysis With a Proposed Job Analyzer Component based on Stack Inspection Methodology", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 1442-1447, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[49] Hisham A. Kholidy, "HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra", The 2nd International Conference on Computer Technology and Development ICCTD, pp 163-168, Cairo, 2010.

[50] R. Bohn, A. Battou, B. Choi, R. Chaparadza, S. Song, T. Zhang, T. Choi, Hisham A. Kholidy, M. Park, S. Go, “NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking”, in the IEEE Future Networks World Forum (FNWF), 13–15 November 2023 // Baltimore, MD, USA.

[51] I. Elgarhy, A. El-toukhy, M. Badr, M. Mahmoud, M. Fouda, M. Alsabaan, Hisham A. Kholidy, “Secured Cluster-Based Electricity Theft Detectors Against Blackbox Evasion Attacks”, in the IEEE 21st Consumer Communications & Networking Conference (CCNC), 6-9 January 2024.

[52] M. C. Zouzou, E. Benkhelifa, Hisham A. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 19-22 June 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.

[53] Hisham A. Kholidy, Andrew Karam, James Sidoran, et al. “Toward Zero Trust Security in 5G Open Architecture Network Slices”, IEEE Military Conference (MILCOM), CA, USA, November 29, 2022. https://edas.info/web/milcom2022/program.html

[54] Hisham A. Kholidy, Andrew Karam, Jeffrey H. Reed, Yusuf Elazzazi, "An Experimental 5G Testbed for Secure Network Slicing Evaluation", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp- content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[55] Hisham A. Kholidy, Riaad Kamaludeen "An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[56] Hisham A. Kholidy, Salim Hariri, "Toward an Experimental Federated 6G Testbed: A Federated leaning Approach", the 19th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2022), Abu Dhabi, UAE December 5th - December 7th, 2022

[57] Hisham Kholidy, Andrew Karam, James L. Sidoran, Mohammad A. Rahman, "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", the 26th IEEE Symposium on Computers and Communications (The 26th IEEE ISCC), Athens, Greece, September 5-8, 2021. https://ieeexplore.ieee.org/document/9631531

[58] N. I. Haque, M. Ashiqur Rahman, D. Chen, Hisham Kholidy, "BIoTA: Control-Aware Attack Analytics for Building Internet of Things," 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON), 2021, pp. 1-9, doi: 10.1109/SECON52354.2021.9491621.

[59] Samar SH. Haytamy, Hisham A. Kholidy, Fatma A. Omara, "Integrated Cloud Services Dataset", Springer, Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, 18-30. Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA.

[60] Hisham A. Kholidy, Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, "Attacks Detection in SCADA Systems Using an Improved Non- Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), published in February 2018.

[61] Stefano Iannucci, Hisham A. Kholidy Amrita Dhakar Ghimire, Rui Jia, Sherif Abdelwahed, Ioana Banicescu, "A Comparison of Graph-Based Synthetic Data Generators for Benchmarking Next-Generation Intrusion Detection Systems", IEEE Cluster, Sept 5 2017, Hawaii, USA.

[62] Qian Chen, Hisham A. Kholidy, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017.

[63] Hisham A. Kholidy, Abdelkarim Erradi, "A Cost-Aware Model for Risk Mitigation in Cloud Computing Systems", 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[64] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, "Attack Prediction Models for Cloud Intrusion Detection Systems", in the International Conference on Artificial Intelligence, Modelling and Simulation (AIMS2014), Madrid, Spain, November 2014.

[65] Hisham A. Kholidy, Ahmed M. Yousouf, Abdelkarim Erradi, Hisham A. Ali, Sherif Abdelwahed, "A Finite Context Intrusion Prediction Model for Cloud Systems with a Probabilistic Suffix Tree", in the 8th European Modelling Symposium on Mathematical Modelling and Computer Simulation, Pisa, Italy, October 2014.

[66] Hisham A. Kholidy, A. Erradi, S. Abdelwahed, "Online Risk Assessment and Prediction Models For Autonomic Cloud Intrusion Prevention Systems", in the "11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, November 2014.

[67] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[68] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A Hierarchical, Autonomous, and Forecasting Cloud IDS", the 5th Int. Conference on Modeling, Identification and Control (ICMIC2013), Cairo, Aug31-Sept 1-2, 2013.

[69] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "HA- CIDS: A Hierarchical and Autonomous IDS for Cloud Environments", Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) Madrid, Spain, June 2013.

[70] Hisham A. Kholidy, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", the 9th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[71] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[72] Hisham A. Kholidy, Chatterjee N., "Towards Developing an Arabic Word Alignment Annotation Tool with Some Arabic Alignment Guidelines", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[73] Hisham A. Kholidy, Khaled S. Algathber, "A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN", 5th Int. Conference on Information Assurance and Security, Aug 2009, China.

[74] Hisham A Kholidy, A. Azab, S. Deif, "Enhanced ULTRA GRIDSEC: Enhancing High- Performance Symmetric Key Cryptography Schema Using Pure Peer-to-Peer Computational Grid Middleware (HIMAN)", IEEE-ICPCA (the 3rd Int. Conf. on Pervasive Computing and Applications, 06-08 Oct 2008.

[75] A. Azab, Hisham A Kholidy, "An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids", International Conference on Computer Engineering & Systems Nov 2008.
[76] Mostafa-Sami M., Safia H D., Hisham A Kholidy, "ULTRAGRIDSEC: Peer-to-Peer Computational Grid Middleware Security Using High-Performance Symmetric Key Cryptography" in IEEE-ITNG (5th Int. Conf. On Information Technology-New Generations), LasVegas, Nevada, USA, 7-9 April 2008.
[77] Mohammed Arshad, Patel Tirth, Hisham Kholidy, "Deception Technology: A Method to Reduce the Attack Exposure Time of a SCADA System", https://dspace.sunyconnect.suny.edu/handle/1951/70148,
[78] Akshay Bhoite, Diwash Basnet, Hisham Kholidy, "Risk Evaluation for Campus Area Network", https://dspace.sunyconnect.suny.edu/handle/1951/70162
[79] Malkoc, M., & Kholidy, H. A. (2023). 5G Network Slicing: Analysis of Multiple Machine Learning Classifiers. ArXiv. /abs/2310.01747.
[80] Fathy M. Mustafa, Hisham A. Kholidy, Ahmed F. Sayed et al. Distributed Backward Pumped Raman Amplifier Gain Enhancement: New Approaches, 06 April 2023, available at Research Square [https://doi.org/10.21203/rs.3.rs-2770728/v1]
[81] Grippo, T., & Kholidy, H. A. (2022). Detecting Forged Kerberos Tickets in an Active Directory Environment. arXiv. https://doi.org/10.48550/arXiv.2301.00044
[82] Zielinski, D., & Kholidy, H. A. (2022). An Analysis of Honeypots and their Impact as a Cyber Deception Tactic. arXiv. https://doi.org/10.48550/arXiv.2301.00045
[83] Kholidy, H. A., & Abuzamak, M. (2022). 5G Network Management, Orchestration, and Architecture: A Practical Study of the MonB5G project. arXiv. https://doi.org/10.48550/arXiv.2212.13747
[84] Abuzamak, M., & Kholidy, H. (2022). UAV Based 5G Network: A Practical Survey Study. arXiv. https://doi.org/10.48550/arXiv.2212.13329
[85] Kholidy, H. A., Rahman, M. A., Karam, A., & Akhtar, Z. (2022). Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform. arXiv. https://doi.org/10.48550/arXiv.2201.00484
[86] Kholidy, H. A. (2021). State Compression and Quantitative Assessment Model for Assessing Security Risks in the Oil and Gas Transmission Systems. arXiv. https://doi.org/10.48550/arXiv.2112.14137
[87] Kholidy, H. A. (2021). A Triangular Fuzzy based Multicriteria Decision Making Approach for Assessing Security Risks in 5G Networks. arXiv. https://doi.org/10.48550/arXiv.2112.13072
[88] Haque, N. I., Rahman, M. A., Chen, D., & Kholidy, H. (2021). BIoTA Control-Aware Attack Analytics for Building Internet of Things. arXiv. https://doi.org/10.48550/arXiv.2107.14136
[89] Kholidy, H. A. (2020). Cloud-SCADA Penetrate: Practical Implementation for Hacking Cloud Computing and Critical SCADA Systems. Department of Computer and Network Security, College of Engineering, SUNY Polytechnic Institute. http://hdl.handle.net/20.500.12648/1605
[90] Hisham A. Kholidy, Abdelkader Berrouachedi, Elhadj Benkhelifa and Rakia Jaziri, "Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[91] Soufiane Hamadache, Elhadj Benkhelifa, Hisham kholidy,Pradeeban Kathiravelu, Brij B Gupta, "Leveraging SDN for Real World Windfarm Process Automation Architectures", The 10th International Conference on Software Defined Systems (SDS-2023) San Antonio, Texas , USA. October 23-25.
[92] Adda Boulem, Abdelkader Berrouachedi, Marwane Ayaida, Hisham Kholidy and Elhadj Benkhelifa, "A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[93] Meriem Chiraz zouzou, mohamed shahawy, Elhadj Benkhelifa and Hisham Kholidy, "SIoTSim: Simulator for Social Internet of Things", The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.
[94] Hisham A. Kholidy, Keven Disen, Andrew Karam, Elhadj Benkhelifa, Mohammad A. Rahman, Atta-Ur Rahman, Ibrahim Almazyad, Ahmed F. Sayed and Rakia Jaziri, "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[95] Ibrahim Almazyad, Sicong Shao, Salim Hariri and Hisham Kholidy, "Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis and Evaluation", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[96] Abdulbast A Abushgra, Hisham A Kholidy, Abdelkader Berrouachedi and Rakia Jaziri, "Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[97] Adda Boulem, Cyril De Runz, Hisham Kholidy, Abdelmalek Bengheni, Djahida Taib, Marwane Ayaida, "A New Classification of Target Coverage Models in WSNs, Survey and Algorithms and Future Directions", The 7th International Conference on Information and Computer Technologies (ICICT 2024), March 15-17, Honolulu, Hawaii.