AWS, Azure, and Oracle Cloud: A comparative analysis of Open Ports.

GEORGIOS EVANGELOU

Cloud computing is rapidly transforming the IT landscape. Because of this rapid change and adoption it is crucial and necessary to acquire a deep understanding of the technical infrastructure and characteristics of the leading providers in this space. This research focuses on examining the most commonly used open ports in Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud in order to provide a detailed analysis of their technical infrastructure. By assessing open ports at both the provider level and across individual services such as EC2, S3 and Cosmos DB, this study aims to uncover different patterns in port use among these providers. By carrying out a detailed exploration of port configurations and usage, the research seeks to enhance the understanding of cloud infrastructure, offering important insights for stakeholders. The findings of this study can inform decisions and actions regarding cloud architecture, performance optimization, and security measures, in this way aiding in the effective and efficient adoption of cloud services.

Additional Key Words and Phrases: Cloud Computing, Oracle Cloud, Microsoft Azure, AWS, Open Ports, Port Utilization, Cloud Architecture, Cloud Infrastructure, Cloud Services

1 INTRODUCTION

1.1 Network Ports

Open ports are specific endpoints in networks that allow data to enter and exit a network, having an important role in network communication by making possible the transfer of information between different devices and services. Each open port is identified by a different number, ranging from 0 to 65535, which determines how network traffic is directed. For example, port 80 is used for HTTP traffic, while port 443 is used for HTTPS traffic.

Ports act as gates, directing data to the correct application or service on a network device. When a device receives data, it looks at the port number to recognize which application should take care and handle that data. Each port is typically linked with a specific service, for example, port 25 is used for the Simple Mail Transfer Protocol to send emails, and port 53 is used for the Domain Name System services.

1.2 Cloud Computing

Cloud computing is a paradigm that allows for the delivery of computing services, such as storage, processing power, and application, over the internet, often referred to as "the cloud." Cloud computing enables organizations and individuals to use technology resources without the need for significant physical infrastructure. Instead of maintaining physical servers and data centers, users can utilize the cloud provider's infrastructure to deploy, manage, and scale their applications and services.

Author's address: Georgios Evangelou.

In cloud computing, services are delivered over the internet, with open ports playing a vital role in their functionality. Providers such as AWS, Azure, and Oracle Cloud offer numerous services that depend on specific ports to operate. Understanding and managing open ports is critical for maintaining an efficient network, particularly in the complicated and data-intensive realm of cloud computing. By analyzing the open port configurations of major cloud providers, we can have a deeper look on their network infrastructure and enhance our strategies for cloud deployment.

2 PROBLEM STATEMENT AND MOTIVATION

The configuration and the use of open ports is an important aspect of cloud infrastructure that needs further research. Without a detailed understanding of the open port patterns employed by big cloud providers, stakeholders may face challenges in optimizing their cloud deployments, in this way leading to performance issues, inefficiencies, and missed opportunities

2.1 Security

The fast adoption of cloud computing has made it very important for organizations to ensure their cloud environments are secure. Open ports, which serve as gateways for data flow in and out of a network, play a critical role in the security of cloud services. Not configuring properly or poorly understood port configurations can create vulnerabilities that people with malicious intentions might try to take advantage of, leading to data breaches and other security incidents.

2.2 Complexity and Configuration

Each cloud provider has a different set of services with specific port requirements and configurations. A study revealing these patterns can reveal how these services work on a more technical level, manage their traffic of data. This understanding is vital for managing the complexity of cloud infrastructures.

2.3 Decision-Making and Cost Efficiency

The findings of this research can help the stakeholders with making more informed decisions about cloud architecture and management. Optimizing port configurations can enhance cloud performance, improve security, and therefore achieve greater cost efficiencies.

3 RESEARCH QUESTION

Based on the above problem statement, we formed the following main research question and two sub-research questions to help us answer the main research question.

3.1 Main Research Question

- What are the most commonly utilized open ports across AWS, Azure, and Oracle Cloud, and what differences or similarities in port utilization can be identified among these providers?

3.2 Sub Research Questions

- What are the most popular services offered by AWS and Azure, what are the most utilized open ports by these services, and why are these ports essential for their operation?

- What are the most commonly utilized open ports across the entire platforms of AWS, Azure, and Oracle Cloud, and how do the percentages of these open ports compare among the three providers?

4 RELATED WORK

Research on open port configurations and their impact on cloud infrastructure performance and security has been extensively covered, providing a solid foundation for understanding the importance of proper port management in cloud environments.

4.1 Security Implications

H.-C. Li et al. (2010) conducted an analysis on cloud-based security vulnerability assessment, emphasizing the critical nature of managing open ports to prevent vulnerabilities that could be exploited by malicious actors. This study highlights the necessity of securing open ports to prevent unauthorized access and data breaches in cloud environments [4].

4.2 Performance and Optimization

Feroz Zahid (2017) explored network optimization techniques to enhance the performance of high-performance cloud computing. The study emphasized the importance of optimizing network configurations, including open ports, to achieve high efficiency and performance in cloud environments. Zahid's research provides insights into how proper management of open ports can lead to significant improvements in cloud service delivery and performance [15].

4.3 Resource Management in Cloud Computing

Nzanywayingoma and Yang (2018) reviewed efficient resource management techniques in cloud computing environments, discussing various strategies for effective allocation and utilization of resources. Their study highlighted the critical role of proper port configuration in optimizing resource management, thereby enhancing cloud performance and cost efficiency. This emphasizes the necessity of understanding port utilization patterns to manage cloud resources effectively [9].

In the existing literature, there seems to be a gap regarding the patterns and distribution of open ports across the major cloud providers. This study aims to cover this gap by providing a comparative analysis of open port configurations in AWS, Azure, and Oracle Cloud. By uncovering these patterns, we seek to further enhance the understanding of cloud infrastructure.

5 METHODOLOGY

5.1 Censys Dataset

To analyze the port configurations of these three cloud providers, Amazon, Azure, and Oracle, we used a dataset from Censys. Censys is a cybersecurity platform that operates like a search engine, collecting information about devices exposed to the Internet. This platform continuously scans the Internet gathering data on device configurations. This data includes operating systems and software versions, active services and their settings, open ports, and security protocols such as SSL/TLS configurations. Since this dataset was around 3 terabytes, SSH access to a machine hosting this dataset was required.

5.2 Filtering the data

To filter the relevant IP addresses from the Censys dataset, the established IP ranges for the three cloud providers were used[5, 10, 11].

These files organize IP addresses according to specific regions and services to which they belong to.

Regions are the specific geographical locations where providers strategically deploy their infrastructure. This placement across various global locations enhances user access to services and ensures a more reliable experience. To provide more context , some examples of these regions are 'eu-north-1' for AWS, 'aecentral' for Azure, and 'us-ashburn-1' for Oracle Cloud.

Services are the functions provided by the cloud companies. This includes computing power, which supports running applications such as AWS EC2 or Azure Virtual Machines, solutions for data storage like AWS S3 or Azure Blob Storage and networking features that securely link data centers and services such as Azure traffic manager. These offerings are designed to be adaptable and scalable, therefore they can expand according the needs of their users.

Given the huge number of IP addresses and the large size of the dataset, a sampling method was necessary to ensure the file sizes were manageable and representative. For both AWS and Azure, we've allocated 100 IP addresses per each service. This allocation spans across all available regions within each service, this way we ensured a comprehensive and unbiased coverage across our dataset. For Oracle Cloud, since the data regarding the distribution of their IP addresses was not organized by the services that are offered, we selected 100 IP addresses from all the available regions.

Using these filtered IP addresses, matching entries were selected from the Censys dataset. The filtering process focused on selecting the open ports used with these entries. The analysis was conducted at two levels: the general provider level for all the providers and the service-specific level for AWS and Azure.

6 RESULTS

After filtering the IP addresses, we were able to identify 6030 entries of open ports linked with their IP addresses: 989 entries belonged to Oracle, 3889 to Azure, and 1152 to AWS. We then further organized the data into their respective services for AWS and Azure.

6.1 AWS and Azure services and their found instances.

Tables 1 and 2 display the top 30 and 13 most popular Azure and AWS services respectively, based on the number of instances found.

Service	Instances
AzureEventHub	1087
azure_eventhub_data	831
Azure Cosmos DB	605
Azure Service Bus	532
Azure App Service	391
StorageSyncService	383
WVD Relays	290
Azure Virtual Desktop	235
GatewayManager	216
Azure Monitor	181
Azure Devops	164
Azure Front Door	135
AzureSQL	125
Service Fabric	104
Azure Update Delivery	99
AzureIoHub	89
Azure API Management	85
One DS Collector	75
SQL Management	73
Trident Kusto	64
Azure Storage	64
Microsoft Azure Fluid Relay	62
PowerBI	62
AzureSpringCloud	62
Dynamic365 Business Central	56
Azure Connectors	53
Azure Portal	52
AzureArcInfrastructure	51
Dynamic 365 For Marketing Email	42
Cognitive Services Management	39

Table 1. Azure Services ordered by found Instances

Service	Instances
DYNAMODB	210
MEDIA PACKAGE V2	180
S3	177
EBS	144
CLOUDFRONT	144
EC2	99
ROUTE53	72
KINESIS VIDEO STREAMS	51
WORKSPACES GATEWAYS	45
GLOBALACCELERATOR	18
CHIME VOICECONNECTOR	6
CHIME MEETINGS	3
AMAZON	3

Table 2. AWS Services ordered by found instances

Service	Ports and Frequencies
WORKSPACES GATEWAYS	41712: 36, 4195: 6, 22: 3
EBS	443: 144
CHIME MEETINGS	443: 3
GLOBALACCELERATOR	80: 15, 443: 3
DYNAMODB	443: 105, 80: 105
CHIME VOICECONNECTOR	5062: 3, 5061: 3
MEDIA PACKAGE V2	443: 180
AMAZON	443: 3
EC2	80: 75, 443: 15, 22: 6, 3306: 3
CLOUDFRONT	443: 72, 80: 72
S3	80: 105, 443: 42, 444: 24, 460: 6
ROUTE53	53: 72
KINESIS VIDEO STREAMS	443: 51

Table 3. AWS services and their open ports

6.2 Most Popular Azure and AWS Services and their open ports

Tables 3 and 4 present the ports utilized by some of the most popular services offered by AWS and Azure, respectively. For demonstration purposes, we will explain the top three services for each of the two cloud providers in regards to their open ports. For Azure, these services are Azure Event Hub, Azure Cosmos DB, and Azure Service Bus. For AWS, the top services are DynamoDB, MediaPackage V2, and S3.

6.2.1 Event Hub. Azure Event Hubs is a native data-streaming service in the cloud that can stream millions of events per second, with low latency, from any source to any destination. Event Hubs is compatible with Apache Kafka. It enables you to run existing Kafka workloads without any code changes[6].Commonly used ports include 443 (66 instances) for interacting with the service interface through the browser [12]. The port 9093 (60 instnaces) is responsible for the Kafka connections[3], and 5671/5672 (60) for AMQP [13], which handles real-time messaging. Other unassigned ports like 10401-10424 are used for other specific internal services of this service.

6.2.2 Cosmos Database. The Azure Cosmos DB service is a multi-model database service . It supports multiple data models such as documents, JSON files , column like, and graphs. It also provides strong guarantees for its performance and reliability. It ensures it can handle a certain amount of data traffic smoothly. [7] Port 443 (43) is used for HTTPS communication conducted in the web browser. The other ports 12202 (32), 12502, 12203, etc. support internal services such as data replication, resource management, and inter-node communication.

6.2.3 Service Bus. Azure Service Bus is a messaging service that enables communication between applications and services. It supports complex messaging patterns while ensuring message delivery even if the receiving service is not available. It provides features like message queues and topics in order to provide efficient and reliable delivery of messages [8]. Regarding the common ports, port 443 (63 instnaces) is the most popular one. The rest of the ports such as

Service	Ports and Frequencies
AzureEventHub	443: 66, 10405: 61, 10402: 61, 10404: 61, 9093: 60, 10401: 60, 5671: 60, 8443: 60, 5672: 60, 10403: 60, 10406: 48, 10409: 42, 10407: 41, 10408: 40, 10412: 35, 10411: 34, 10410: 33, 10413: 29, 10415: 29, 10416: 28, 10414: 27, 10418: 26, 10422: 22, 10424: 22, 10420: 22
Azure Cosmos DB	443: 43, 12202: 32, 12502: 32, 12203: 32, 12200: 32, 11002: 32, 11300: 32, 12503: 32, 11500: 32, 12602: 32, 15502: 32, 12201: 32, 14006: 32, 12504: 32, 12601: 32, 12204: 29, 14330: 29, 12509: 28, 12207: 28
Azure Service Bus	443: 63, 5671: 63, 8443: 63, 5672: 63, 9093: 27, 9402: 24, 9403: 24, 9401: 24, 9404: 24, 9400: 24, 80: 24, 9406: 23, 9407: 23, 9405: 23, 9409: 20, 9408: 20
Azure App Service	443: 98, 80: 98, 1221: 98, 8172: 97
StorageSyncService	443: 206, 446: 41, 444: 41, 546: 24, 646: 24, 746: 24, 19084: 23
WVD Relays	443: 96, 80: 96, 454: 95, 22: 2, 111: 1
Windows Virtual Desktop	443: 79, 80: 79, 454: 77
GatewayManager	443: 42, 8443: 42, 10443: 42, 9443: 42, 11443: 24, 12443: 24
Azure Monitor	443: 43, 80: 30, 9100: 20, 8902: 20, 8952: 20, 9201: 20, 1886: 20, 8082: 1, 28686: 1, 10002: 1, 8081: 1, 8444: 1, 10001: 1, 20000: 1, 8443: 1
Azure Devops	443: 55, 80: 55, 22: 54
Azure Front Door	443: 46, 80: 45, 53: 44
AzureSQL	11506: 7, 11023: 7, 11001: 7, 11519: 7, 11002: 7, 11004: 7, 11009: 6, 11025: 6, 11013: 6, 11007: 6, 11510: 6, 11508: 6, 11513: 6, 11514: 6, 11517: 6, 11000: 6, 11024: 6, 11507: 6, 11002: 6, 11022: 6, 11003: 6
Service Fabric	443: 52, 10021: 52
Azure Update Delivery	443: 78, 80: 17, 22: 1, 6391: 1, 6390: 1, 3443: 1
AzureIoHub	443: 26, 8883: 25, 5671: 25, 9999: 9, 9555: 1, 8001: 1, 80: 1, 16001: 1
Azure API Management	443: 29, 3443: 25, 4291: 23, 80: 6, 6391: 1, 6390: 1

Table 4. Azure Services and their open ports

9404, 9400, 9406 etc. are not linked to a specific service but we can assume that they support its internal services.

6.2.4 DynamoDB. Amazon DynamoDB is a fully managed, NoSQL database service that offers low-latency regarding its performance. It automatically handles database management tasks like setup, scaling, and maintenance. DynamoDB supports key-value and document data models [1]. According to our data the Ports of 443 and 80 were both recorded 105 times. Port 80 is used for HTTP traffic. Initial requests might start on port 80 [14]and then be redirected to HTTPS for enhanced security.

6.2.5 MEDIA PACKAGE V2. MediaPackage v2 is a video streaming service. It integrates with other AWS services such as MediaLive and CloudFront [2]. The data recorded indicates that MediaPackage v2 exclusively uses port 443 with its operations, with 180 recorded instances.

6.2.6 Amazon S3. Amazon S3 is a scalable and high-speed web-based cloud storage service designed for online backups and archiving of data and applications. It offers object storage through a web interface. The collected data shows that Amazon S3 uses port 80 (105 instances) for HTTP for non-secure communication, typically for less sensitive data or initial requests. Port 443 (42) is used ensuring secure and encrypted communication when interacting with the services interface. Ports 444 and 460 are also recorded.

In general, a deeper examination of port distribution for each service offered by the two cloud providers reveals a common pattern: the most popular ports are 443 and 80. This is expected, as these ports are commonly used for interfaces that allow users to interact with the services through the web browser. Additionally, we observe a lower number of instances for other open ports, which are used for specific technical requirements of the services. Understanding the exact purpose of each open port can be challenging, as it is determined by the cloud provider's specific implementation and needs.

6.3 Most common open ports for AWS and Azure and the number of service instances for each port

The fig. 1 presents a bar chart showing the distribution of service instances across the most popular network ports of AWS, showing both the ports and the number of instances for each service. Port 443 is the most used with a total of 618 instances, filling EBS (144), MEDIA PACKAGE V2 (180), DYNAMODB (105), CLOUDFRONT (72), KINESIS VIDEO STREAMS (51), S3 (42), AMAZON (3), GLOBALACCELERATOR (3), and CHIME MEETINGS (3). Port 80 is the next most used with a total of 372 instances, used mostly by DYNAMODB (105), S3 (105), CLOUDFRONT (72), EC2 (75), and GLOBALACCELERATOR (15). Port 53 (72) is used only by ROUTE53. Then we have port 41712 (36) which is exclusively used by the Workspace Gateways service. The Port of 444 (24) is used by S3.

The fig. 2 presents the same bar chart showing the share of service instances with the most popular network ports used by Azure. First, we have Port 443 which is the most utilized with a total of 479 instances, inhabited by StorageSyncService (206), Azure App Service (98), WVD Relays (96), and Windows Virtual Desktop (79). Port 80 is next having 318 instances, used by Azure App Service (98), WVD Relays (96), Windows Virtual Desktop (79), and Azure Front Door (45). Then there is Port 454 with 183 instances, used by WVD Relays (95), Windows Virtual Desktop (77), and Azure Connectors (11). Port 8443 is next with 176 instances, used by Azure Service Bus (63), azure eventhub data (60), GatewayManager (42), and Azure

Storage (11). Port 5671 is shown in 148 instances, used by Azure Service Bus (63), azure eventhub data (60), and AzureIoHub (25).

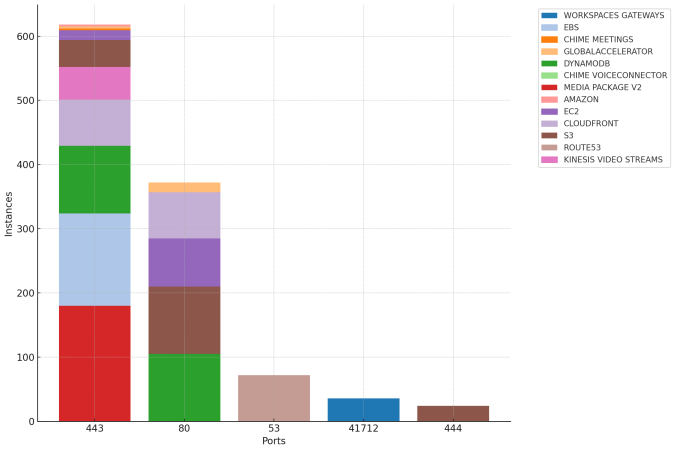

Fig. 1. AWS Service Instances by the most popular ports.

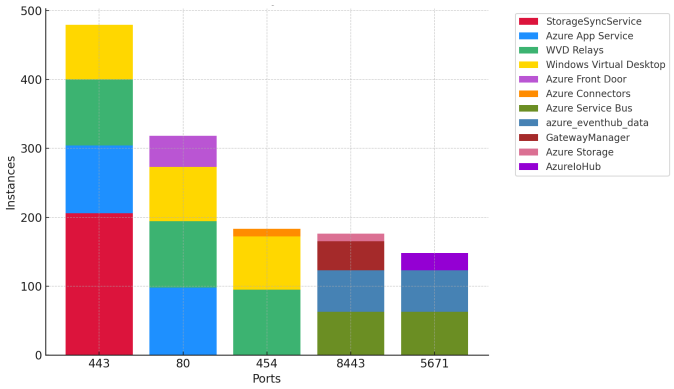

Fig. 2. Azure Service Instances by the most popular ports.

6.4 General Port Distribution for AWS, Azure and Oracle

Fig.3 illustrates the distribution of the most common ports used in the Oracle network. Port 443 is the most commonly used, accounting for 45.9% of the activity. It is followed by Port 22 with 23.9%, and Port 80, which is used for 13.7% of the connections. Port 111 comes next at 4.3%, followed by Port 8443 with 1.4%, and Port 8080 at 1.3%. Further down the list, Port 21 and Port 6443 each account for 0.9% of usage. Ports 9000, 3389, 25, and 123 each represent 0.7%, while Port 12250 and 465 each make up 0.6%. Ports 53, 2083, 20000, and 43080 each have a 0.5% share, and the least common in this summary, Ports 3306, 5000, 5244, and 9527, each hold 0.4% of the usage.

Fig. 4 shows the distribution of port usage in the AWS cloud. Port 443 leads with 53.6 precent, followed by port 80 at 32 precent, and port 53 at 6.2 %. Other notable ports include 4172 at 3.1% 444 at 2.1% 22 at 0.8% and various others like 460, 4195, 3306, 5062, and 5061, each around 0.3-0.5%

Fig.5 illustrates the distribution of port usage within Azure. Port 443 dominates with 43.4% followed by port 80 at 15.7%. Other significant ports include 454 and 8443, each at 4.5%, and 5671 and 5672, both at 3.6%. Additional ports like 1221 and 8172 are used at 2.4%, with 9093 at 2.1%. Lesser-used ports such as 1433, 10405, 10402, 10404, and 10401, each at 1.5%, along with 10403, 10021, 10443, 10406, 53, 9443, 444, 25, and 10409, all range from 1.0% to 1.3%.

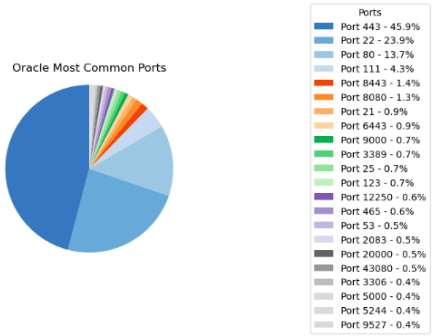

Fig. 3. General port distribution for Oracle cloud

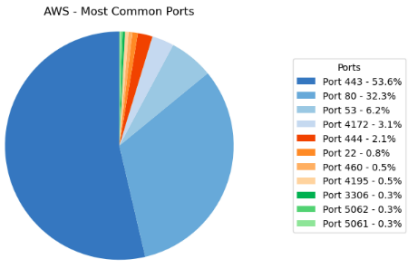

Fig. 4. General port distribution for AWS cloud

7 CONCLUSION AND FUTURE WORK

This research demonstrated the distribution of open ports on a service-specific level for AWS and Azure, and on a more general level for AWS, Oracle, and Azure. These findings can be very useful for cloud architects, security specialists, and stakeholders interested in understanding cloud computing on a more technical level.
For future work, it would be very valuable to dive deeper into the security implications of the open ports identified in this study and investigate possible security vulnerabilities associated with them. This could provide deeper insights into how these vulnerabilities

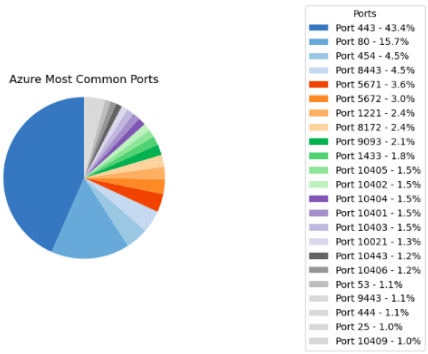

Fig. 5. General port distribution for Azure cloud

can be avoided in order to enhance the overall security of cloud infrastructures.

8 USE OF CHATGPT

During this research the author used the assistance of ChatGPT for data analysis and to improve the grammar and writing quality of the thesis. . After using this tool, the author reviewed and edited the content as needed and takes full responsibility for the content of the work.

REFERENCES

[1] Amazon Web Services. 2024. Amazon DynamoDB Documentation. https://docs.aws.amazon.com/dynamodb/ Accessed: 2024-07-07.
[2] Amazon Web Services. 2024. AWS Elemental MediaPackage Documentation. https://docs.aws.amazon.com/mediapackage/ Accessed: 2024-07-07.
[3] Apache Software Foundation. 2024. Apache Kafka Documentation. https://kafka.apache.org/090/documentation.html Accessed: 2024-07-07.
[4] Huan Chung Li, Po Huei Liang, Jiann Min Yang, and Shiang Jiun Chen. 2010. Analysis on cloud-based security vulnerability assessment. In *Proceedings - IEEE International Conference on E-Business Engineering, ICEBE 2010 (Proceedings - IEEE International Conference on E-Business Engineering, ICEBE 2010).* 490–494. https://doi.org/10.1109/ICEBE.2010.77 IEEE International Conference on E-Business Engineering, ICEBE 2010 ; Conference date: 10-11-2010 Through 12-11-2010.
[5] Microsoft. 2023. Microsoft Azure Datacenter IP Ranges. https://www.microsoft.com/en-us/download/details.aspx?id=56519 Accessed: 2024-07-07.
[6] Microsoft Azure. 2024. About Azure Event Hubs. https://learn.microsoft.com/en-us/azure/event-hubs/event-hubs-about Accessed: 2024-07-07.
[7] Microsoft Azure. 2024. Azure Cosmos DB. https://azure.microsoft.com/en-us/products/cosmos-db Accessed: 2024-07-07.
[8] Microsoft Azure. 2024. Azure Service Bus Messaging. https://learn.microsoft.com/en-us/azure/service-bus-messaging/ Accessed: 2024-07-07.
[9] Frederic Nzanywayingoma and Yang Yang. 2017. Efficient Resource Management techniques in Cloud Computing Environment: A Review and discussion. *Telkomnika (Telecommunication Computing Electronics and Control)* 15 (12 2017), 1917–1933. https://doi.org/10.12928/TELKOMNIKA.v15i4.6574
[10] Oracle. 2023. Oracle Cloud Infrastructure Public IP Ranges. https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json Accessed: 2024-07-07.
[11] Amazon Web Services. 2023. AWS IP Address Ranges. https://ip-ranges.amazonaws.com/ip-ranges.json Accessed: 2024-07-07.
[12] SpeedGuide.net. 2024. Port 443 Details. https://www.speedguide.net/port.php?port=443 Accessed: 2024-07-07.
[13] SpeedGuide.net. 2024. Port 5671 Details. https://www.speedguide.net/port.php?port=5671 Accessed: 2024-07-07.
[14] SpeedGuide.net. 2024. Port 80 Details. https://www.speedguide.net/port.php?port=80 Accessed: 2024-07-07.
[15] Feroz Zahid. 2017. Network Optimization for High Performance Cloud Computing. https://api.semanticscholar.org/CorpusID:49378993