BEST JOURNAL OF INNOVATION IN SCIENCE, RESEARCH AND DEVELOPMENT
ISSN: 2835-3579
Volume:1 Issue:3 | 2022
www.bjisrd.com

Zero-Trust Access Control Systems by Artificial intelligence in Hybrid Cloud Environments

Lamia Akter
Bachelor of Science in Computer Science & Engineering, Ahsanullah University of Science and Technology

Dr. Muhammad Mainuddin Mollah
Associate Professor, Institute of Social Welfare & Research, University of Dhaka

Nusrat Jahan Sany
Southeast University, Bachelor of Business Administration, Major in Accounting

Sagor Ahamed
Bachelor of Science in Computer Science & Engineering, Ahsanullah University of Science and Technology

Abstract**:** *As cybersecurity attacks get more advanced and are delivered from more distant sources, perimeter-based security is not enough for hybrid cloud environments. Because of the increasing complexity and sharing of IT systems, traditional controls placed at a company's edges do not work well in hybrid cloud setups. As a result, Zero-Trust Access Control Systems (ZTACS) have become a key solution, working by assuming nothing and always verifying identity. This work studies how to use AI in Zero Trust frameworks to make access control, detect abnormalities, and ensure policies are properly enforced in the ever-changing cloud environment. The Hornet 40: The research uses the Network Dataset of Geographically Placed Honeypots as its main evidence and data. In this dataset, information collected using 40 honeypots scattered around the world is used to spot malicious behavior and attempts at unauthorized access. Using the dataset, Random Forest, Isolation Forest, and Autoencoders help model patterns of behavior, find anomalies, and determine how risky user access is in real time. The analysis reveals that using AI with ZTACS helps to spot unusual access behaviors more quickly and with fewer false alarms than other approaches. Using dynamic trust scoring and behavior-based authentication leads to improved accuracy in making access choices that do not slow down operations in a hybrid cloud environment. It also points out some major challenges*

when using AI for security, including unbalanced sets of threats, difficulties in understanding how models work, and ensuring that data is protected. This work provides information on the technical benefits of AI-driven Zero Trust systems in facing cyber threats in distributed environments. These findings encourage developing access control systems that are automated, scalable, and use artificial intelligence to meet the needs of current cloud security. Uniting Zero Trust principles with AI could be the future of company cybersecurity.

Keywords: *Zero Trust Architecture (ZTA), AI-Powered Access Control, Hybrid Cloud Security, Network Anomaly Detection, Honeypot-Based Threat Analysis and Cybersecurity Automation.*

1. Introduction

1.1 Background

The rise of digital transformation is encouraging different businesses to use hybrid cloud, which is made up of on-site hardware and both private and public cloud services. While a mix of on-premises and cloud platforms ensures that more can be done flexibly and cost-effectively, it comes with new challenges regarding security that classic models can't handle. Because hackers now use a wide range of techniques, including those from within an organization, access control methods must be updated for any organization with distributed computing [1]. Once-useful perimeter security is not as good at handling advanced threats that can enter a system from within and easily use assumed trust. For these organizations, the combination of decentralized data centers, changing workloads, and routine use of third-party services makes it necessary to often verify who is accessing the system, the security of the device, and the reason for access. Because work is now done from many places and on different devices, the network boundary no longer exists, which means old security policies don't work. As a result of these changes, it is now important to have smart, aware, and action-focused security approaches that can respond instantly in different situations [2]. As cyber attackers start using automation and AI to beat existing defenses, security must advance as well by using advanced detection, analytics, and flexible controls. When supported by AI, Zero Trust Architecture (ZTA) introduces a new approach to cybersecurity, allowing for flexible and risk-based access control as the security situation in hybrid cloud environments changes [3]. This research focuses on how AI enables ZTACS to work well, pointing out that standing up to threats in real-time and supporting security over extensive global networks is key. The use of machine learning on honeypot data offers useful information on recent threats and how AI can help tackle them.

1.2 Explain the meaning of Zero Trust (ZTA) and Hybrid Cloud Environments

ZTA stands for Zero Trust Architecture, which is based on the belief of "never trust, always verify." Instead of believing everything inside the network is trustworthy, as traditional security does, ZTA considers that both the internal and external networks might get compromised [4]. All permission requests are checked at every stage using information about the user, their device, their current location, and typical behavior. In this way, ZTA aims to minimize the exposure of a system by using strict policies, requiring repeated logins, restricting access, and dividing network resources. Zero Trust approach depends on various tools like MFA, IAM, behavioral analytics, and segmenting the network. Rather, hybrid cloud involves running IT systems on-site as well as in public and private clouds so that businesses can make use of the benefits of each deployment option [5]. While hybrid clouds are flexible, cost-effective, and scale well, their dispersed and shifting architecture introduces distinct

security issues. Resources and users can be in many different places and systems, which makes it hard to keep everything secure, clear to see, and in line with all the rules. By adopting Zero Trust with hybrid clouds, security decisions are guided by current risks and factors, and not just on previously established identity or where the user is located. When it is put into place right, ZTA ensures all parts of a hybrid infrastructure have the same security rules, no matter if they are on-site or in the cloud. ZTA plus hybrid cloud brings a forward-thinking way to handle security by addressing the recent problems of identity, trust, and control in IT environments [6]. This paper looks at how Zero Trust and AI can bring together intelligent, adaptive, and scalable methods for managing access in hybrid cloud systems.

1.3 Describe the Constraints of Using Network Perimeters for Security Measures

Traditional security models for networks assume that all external factors are threats, and everything within the network is completely trusted. Firewalls, VPNs, and IDS systems are key tools that help protect the internal network through a ring of security [7]. Recent advancements in IT, such as more cloud-based services, have rendered these models less reliable. There are more holes in the perimeter today due to the increasing use of cloud, mobile devices, remote work, and third-party software. Attackers can easily move laterally inside the network once they have broken through the outer security, since their movement is rarely detected. These kinds of models don't consider that insider threats are a significant risk because they come from trusted sources [8]. Static access policies do not respond to new user actions or situation changes, leaving companies more at risk of having their credentials stolen or misused. The fact that authentication does not always happen in the same way and decisions are not based on the environment prevents the model from handling today's most significant attacks, such as zero-day attacks, phishing attacks, and the threat of ransomware [9]. One more challenge is that in a hybrid cloud, the data and applications are spread across various platforms, causing challenges for old systems. Security policies cannot be easily maintained and kept visible in fragmented IT places with only a perimeter firewall. Besides, these models require manual handling and do not react swiftly to new dangers, so responses are slow. As cyber attackers rely on automation and complex methods, standing still and responding to attacks is not enough anymore. Zero Trust and similar models based on granular security, dynamism, and identity are vital for securing today's company networks.

1.4 Explain Why AI is Vital for Handling Access Control in a Flexible and Real-Time Managed Way

In the field of cybersecurity, AI is particularly useful for protecting access control, thanks to its ability to make real-time and flexible choices. Since being secure is constant in ZTA, AI is used to analyze lots of data, notice anomalies, and let policies be applied automatically [10]. Older rule-based approaches struggle to keep up with fast-changing and new safety concerns. In comparison, machine learning and deep learning models in AI can track normal actions, spot any unusual activity, and safeguard against risks with little need for human direction. AI takes in network telemetry, log data, user behavior, and device health measures to calculate updated trust scores in real time. The scoring is used to help decide if access is allowed based on factors such as the time, place, and how often the resource is accessed. When systems are hybrid, which means there are many platforms being used and user contexts vary, AI allows for the scale required to keep security policies steady. It further allows faster finding and control of problems related to insiders, unauthorized use of credentials, and complex attacks not usually detected. AI-enabled access control systems can focus on important alerts, cut down on unwanted alarms, and always aim to better themselves through feedback. With the help of AI, ZTA allows organizations to stop reacting to threats and become more proactive, quickly identifying

and reacting to them [11]. This degree of intelligence and automation is vital where even a moment of delay could put data at high risk of being exposed. Combining Zero Trust concepts with AI helps secure access in complex IT systems, ensuring there is flexibility and strength in the current state of cybersecurity.

1.5 Analyzing the Role of AI in Enhancing ZTA Inside Hybrid Clouds

This study aims to assess the impact of Artificial Intelligence (AI) on Zero Trust Access Control Systems (ZTACS) in mixed cloud environments. Since hybrid cloud uses many platforms, changes over time, and includes internal and external ways for users to access resources, it brings its own security challenges [12]. To maintain access control in such cases, we need to switch from static policies to systems that adapt in the moment. While the idea of Zero Trust Architecture is solid, it requires strong, fast, and easily scalable rules and systems to work well. They do this by providing behavioral analysis, detecting anomalies, performing dynamic assessments of risks, and automatically following the set policies [13]. This paper explores how machine learning can help analyze actual network traffic patterns, using data from the Hornet 40 dataset that covers traffic from honeypots around the globe. The purpose of this study is to detect differences between authorized and unauthorized access attempts, check the ability of artificial intelligence to predict these attempts, and notice how effective AI is in enforcing the principles of Zero Trust security. When setting up hybrid clouds, extra effort is given to ensure good accuracy, how adaptable the models are, and how well they can be scaled [14]. It also investigates the problems and moral issues involved in using AI-based access controls, covering privacy concerns, understanding how models come to their conclusions, and resistance to attacks. Since the study uses actual data and real-world cases, it improves our understanding of how AI can use ZTA to defend important resources in IT infrastructures.

1.6 Research Objectives

The main aim of this study was:

- To understand how AI works within Zero Trust Access Control Systems.
- To investigate the effectiveness of machine learning at finding unusual access to IT resources.
- To determine how well AI-based access control works when connected to multiple cloud environments [15].
- To display how dynamic trust scoring can improve the process of who has access to certain information.
- To understand the problems and boundaries of using AI in access management right now.
- To develop a model framework for carrying out AI-enhanced ZTA by using data from honeypots.

1.7 Research Questions

This study focuses on these main research questions:

- How successfully can AI-based models spot attempts to access systems under a Zero Trust setup?
- What signals in the network usually indicate that malicious activity will take place in a hybrid cloud environment?
- Is it possible to apply AI-based access controls consistently in many different hybrid cloud environments?
- What things need to be considered when using AI for access control?

2. Literature Review

This section investigates the main ideas and new developments around Zero-Trust Access Control Systems that use AI to work well in cloud environments that mix on-site and cloud resources [16]. It looks at how network security has changed over time, how Zero Trust becomes more important in today's changing workplaces, and how AI helps make security systems quicker and smarter by recognizing who is requesting access and why. Furthermore, it looks at the unique problems that come with protecting a hybrid cloud setup and why making quick decisions in real time really matters [17]. It shows how data from underused websites can be used to teach AI tools to better spot dangerous activity and help keep networks safe.

2.1 The Growth of Network Security and the Impact of Zero Trust

The approach to network security has moved from clinging to a fixed outside boundary to focusing on identity-based defenses. Before, traditional security models believed that the threats came only from the outside world, so they trusted the internal teams completely. Yet, because of more mobile gadgets, shared workplaces, and cloud-computing options, these assumptions are no longer valid [18]. Today, organizations have to deal with threats that come from within and from the outside. As a result, businesses must keep checking identities, device status, and the reason for accessing the system. ZTA fills these gaps by not trusting anyone automatically and validating every attempt to access the system [19]. As a result, new rules can be made to control access, and network activity becomes more transparent. ZTA encourages a security approach that revolves around least privilege, sectioning off data, and immediate monitoring. The design of the system helps it work in situations like the hybrid cloud, since traditional boundaries are no longer in place. Implementing ZTA means joining identity management, analytics of behavior, and device status into a single system. The model relies on assessing risk as it changes, not just on the static credentials alone [20]. Trying to determine the right protection and authentication setting, ZTA keeps changing based on the current risks and the use of the system. Even though Zero Trust does offer many benefits, the process of switching to the model is complicated and usually involves redesigning both the network and security policy systems. However, Zero Trust is becoming more popular because it successfully addresses modern cyber threats, reduces the exposed part of the network, and improves how distributed computing works in case of emergencies.

2.2 Defining the Role of AI in Modern Access Control

Using AI is key to the advancement of access control in environments that distribute and link many computer systems [21]. The current approach to access control does not allow for real-time updates to its policies or rules to cope with quickly evolving risks and new types of user activity. AI gets around this time-consuming way of doing things by using learning systems that look at how people behave, spot unusual activity, and quickly make smart choices as things happen. Through continuous evaluation of login rates, location information, device health, and user behavior, machine learning helps build up to date risk profiles. This way, systems can decide on access by looking at the situation, rather than only using pre-defined roles or user credentials. AI is essential in establishing levels of trust and controlling how policies are applied on the fly in a Zero Trust setting [22]. AI collects information from various sources in hybrid environments and makes it easier to discover patterns that can be missed manually. AI can spot these kinds of threats by learning what normal activity looks like and then alerting when things change in unexpected ways. With this predictive feature, companies can act in advance and quarantine computers at risk or withdraw access to those who should not have it [23]. AI-based identity analytics help verify a person's identity by combining their actions with their

biometric characteristics or surrounding information. Using AI brings benefits only when it is trained with large datasets and checked often to ensure it is making decisions objectively. Although integrating AI in access control comes with difficulties, it still improves the responsiveness of the system, lowers the rate of wrong alarms, and helps enforce Zero Trust policy on different cloud environments.

2.3 Problems Related to Security in Hybrid Cloud Systems

Hybrid cloud environments introduce certain security concerns due to having both public and private cloud sections, many ways to access them, and multiple tenants sharing the cloud. Since these infrastructures can travel across borders and governmental areas, this makes it difficult for security to be overseen and managed properly [24]. This kind of environment requires a new type of security since users and services can be accessed both inside and outside the network. Because there is no central authority, it can be hard to manage policies and enforce the same setup, leading to more issues with settings. Sharing data among multiple cloud providers makes it more vulnerable to vital data being intercepted, used by someone unauthorized, or breaking compliance rules [25]. In addition, using third-party services in hybrid clouds makes it more difficult to keep all components secure. Another major concern is identity sprawl, which makes using one authentication and authorization system over multiple platforms harder. Not connecting different cloud service providers can make it hard to catch threats in real time and slow down reaction. Making endpoint protection work in hybrid environments can be harder as more people use unmanaged devices [26]. It becomes more challenging to use network segmentation when systems and tasks are spread out and always in motion. With hybrid systems in place, traditional static security is not enough and more secure access control is required. To deal with these issues, it is important for organizations to put in place flexible policies that limit what people can access. Security is best maintained in these changing environments by regularly examining and changing the level of trust. For this reason, smart organizations are turning to Zero Trust and AI technology to help create agile and robust security systems that fit hybrid clouds.

2.4 Enhancing Real-Time Decision-Making with AI in ZTA

Real-time decision-making is important when following Zero Trust, because in hybrid cloud environments, things like where people are and what they can get access to change all the time. AI technologies make it possible to quickly work through huge amounts of data, find important patterns, and help make quick and flexible decisions about who can access certain information. In a Zero Trust framework, each time someone tries to access something, it needs to be checked carefully using who they are, what they are doing, and what is happening in the environment [27]. AI systems can quickly look at all these things in just a few milliseconds, making it easy for users to enjoy a smooth experience while keeping everything safe. Real-time analytics with AI help check trust levels all the time by using things like how the device is held, the way a person logs in, unusual locations, and the way data moves on the network [28]. AI models can spot small changes in how people use their accounts, which could mean someone's login details have been stolen or an employee is up to something suspicious, so it might ask for two steps of login or deny certain access. By looking at information from different places on the network, like the devices, users, and the traffic moving across them, AI helps make sure decisions about access are made when considering everything together, not just one thing at a time [29]. This integrated analysis helps us handle security problems faster and cuts down the need for people to fix things manually. In hybrid cloud settings, where workloads often move between different environments, AI helps make sure policies are applied quickly and keep things consistent across everything. Moreover, real-time threat information can be connected to AI to keep control systems updated as new threats come up, making it even faster and safer to check if someone

should be allowed in. However, using AI effectively means making sure it is managed well by having good rules and checks in place, so that people can understand how the decisions are made and know they follow company rules. When used correctly, AI helps Zero Trust systems work smoothly, letting them automatically adjust who has access depending on how risky things get.

2.5 Using data from honeypots to power AI tools for finding threats

Honeypot systems offer malicious actors targets to exploit, while recording all the details of how attacks are carried out. Information gathered from honeypots is crucial for improving AI systems that look for security threats and guard access points [30]. Using honeypot data in Zero Trust and hybrid cloud scenarios messes up unsupervised AI learning by simulating real threats. Analyzing the traffic passing through the network, scanning different ports, and handling brute-force attacks allows AI software to see the difference between useful and harmful activity. For example, the Hornet 40 dataset covers attacks all over the world and supports the production of models that can withstand various evasion techniques based on location. Training AI with these sets of data helps models understand zero-day threats by looking for unusual behaviors instead of using pre-set malware signatures [31]. It helps detect risks quickly and early, something that is very important when fast responses are important. Since honeypot data includes known malicious activity, automated verification of anomaly detection models is made easier. In addition, the information gathered can be included in threat classification systems to decide which incidents receive the most focus during a response [32]. This leads to better and more specific calculation of threats and stronger enforcement of security rules. Regular data flow from honeypot activity helps AI adapt to new types of threats in real time. By feeding honeypot data to the access control system, Zero Trust frameworks become more resistant to threats, aid in advanced threat detection, and adjust their approaches over time.

2.6 Empirical Study

The paper “Advancing the Application of Zero Trust Architecture in Cloud Environment” proposes a new approach. The authors in the 2021 paper "Redefining Zero Trust Architecture in Cloud Networks: A Conceptual Shift Towards Granular, Dynamic Access Control and Policy Enforcement" propose a new model for Zero Trust architecture that more accurately reflects the shifting requirements of cloud networks [1]. The authors contend that static ZTAs are unable to effectively counter the constantly changing risks and dynamic needs of cloud networks. They put forward an advanced architecture that utilizes ongoing risk assessment and enforces policies in real time to improve protection. This proposed framework shares similarities with the goals of our investigation which explores the data collected from the Hornet 40 network. 40 days of attack traffic captured from eight geographically dispersed cloud-based honeypots. The systematic analysis of traffic data from the Hornet 40 dataset confirms the conclusions reached by Ike et al. (2021) regarding the patterns and geographical distribution of cloud threats. The Hornet 40 dataset helps validate the requirement for granular and dynamic access control in Zero Trust systems and highlights the benefit of using context-based policy enforcement for securing hybrid cloud architectures against constantly changing cyberattacks.

The authors explored the security aspects of ZTNA in cloud computing in their paper titled ‘Security of Zero Trust Networks in Cloud Computing’. In 2022, Sirshak Sarkar and his co-authors presented the finds and their implications in the paper “Security of Zero Trust Networks in Cloud Computing: A Comparative Review,” published in Sustainability. The authors present a thorough overview of the development and use of Zero Trust Network Architecture (ZTNA) in cloud computing systems. The authors highlight that traditional perimeter-defense approaches are being superseded by the ZTNA paradigm, which considers all nodes and entities as potentially unsecured and cannot rely on

predefined levels of trust. They comprehensively organize recent ZTNA innovations according to nine critical technical aspects that directly correspond to contemporary cloud environments [2]. Their study documents the need for integrating behavioral reputation assessments, centralized governance, and self-learning threat monitoring into ZTNA deployments. The findings of this study are further validated by this recently published body of work. use Hornet 40, a dataset of geographically spread honeypots, to study the actual differences in threat activity that occur across diverse cloud settings. The Hornet 40 results support the call for flexible, context-aware policies elaborated in Sarkar et al.'s research. This research and the literature review comprehensively support developing and applying flexible Zero Trust models to efficiently counter the diverse cyber threats in modern hybrid clouds.

The article "A Maturity Framework for Enhancing Zero-Trust Security in Multi Access Edge Computing" by Belal Ali et al. explores the creation of a ZTS maturity model for MEC. A customized maturity model is proposed for implementing Zero-Trust Security in MEC environments, which enable service providers to deliver cloud resources at the network edge. The researchers point out that because MEC environments are constantly changing, dispersed and open, conventional situated security strategies no longer satisfactorily protect against modern threats [3]. The framework presents strict security measures consistent with the ZTS approach, requiring continuous evaluation of trustworthiness for all parties interacting in the system. The model advances from a "Minimum Viable Security" level to a "Fully Implemented Security" phase, at which point all interactions are preceded by comprehensive trust verification. The proposed implementation strategy is founded on tried and tested protocols, like NIST 800-207 and MITRE ATT&CK, complemented with hardware-based measures including Physical Unclonable Functions (PUFs) designed to resist sophisticated threats. This study introduces an approach to implement ZTS gradually in MEC and cloud systems. It guides and reinforces the significance of adaptive, well-layered security structures—particularly for processing voluminous and dispersed data reliably collected from the world's leading honeypot cluster, the Hemlock 40 network.

Tackling Modern Cyber Threats by Combining AI and ZTA. Modernizing Cybersecurity by Utilizing AI and ZTA: A Proposal for Combined Adaptability. Traditional security paradigms are becoming obsolete in the face of emerging sophisticated and dynamic cyber security challenges. The paper suggests that integrating AI with ZTA is a major game-changer in the field of cybersecurity. The integration of AI methods like machine learning, anomaly detection, and behavioral analysis allows the Zero Trust model to actively evolve and respond to ever-changing threats in real time. it's shown how integrating AI into ZTA leads to a more effective, flexible, and responsive security posture [4]. Comparison and analysis of available literature reveal that AI-enabled Zero Trust models are highly effective and adaptable for detecting and countering cyber threats. To put development in context, the study outlines how the increase in cyberattacks has coincided with the increasing implementation of AI in security processes. The authors explore how AI-driven zero-trust approaches designed for hybrid cloud environments benefit from the use of datasets such as the Hornet 40 honeypot.

The authors published an article on Zero Trust Access Authorization and Control of Network Boundary Using Cloud Sea Big Data Fuzzy Clustering in the Journal of Intelligent & Fuzzy Systems (2022). The authors propose an innovative solution that combines the advantages of Zero Trust Architecture with sophisticated analytical methods to strengthen security in today's digitally transformed environment [5]. A novel approach for dynamically controlling access by creating a virtual network boundary using network stealth technology is proposed by the researchers. Big data and fuzzy clustering algorithms running on the cloud help the system assess user behavior and determine their trustworthiness. The trust ratings provided to users help decide whether they are

allowed to access specific resources. This approach reveals impressive improvements in both the efficiency and precision of access control at the network periphery. This study introduces a flexible and adaptable security architecture that promotes ZTA concepts through ongoing authentication and limited reliance on an initial level of trust. Using fuzzy logic and big data analytics allows for precise and effective trust assessments in diverse and changing computing environments.

3. Methodology

This study makes use of data and an analytical approach to analyze the importance of Artificial Intelligence for Zero-Trust Access Control Systems in hybrid cloud environments [34]. The methodology follows stages including selecting a dataset, processing the data, building the model, assessing it, and understanding the results

3.1 Dataset Selection

This research employs the Hornet 40: The team is using a network of geographically located honeypots to study the effectiveness of AI-supported Zero-Trust security in hybrid cloud situations [35]. The information in the dataset includes network traffic from honeypots worldwide, covering attacks including port scanning, the distribution of malware, attempts to guess passwords, and attacks that take advantage of well-known security flaws. Because the dataset comes from real-world data and provides a wide range of patterns and activity, it is perfect for training and validating intelligent access control systems. With the wide availability of honeypots, it is possible to test interactions and issues with different global threat actors found in shared cloud environments. It allows for the creation of AI models that can judge the difference between normal and dangerous online actions. Knowing these surfaces and access patterns allows us to see the risks more clearly and enforce the Zero-Trust model. Because the dataset is relevant, the study's analysis looks genuine and is more useful for real world use.

3.2 Data Preprocessing

Reliable and accurate models could only be built by carrying out proper data preprocessing. In the raw Hornet 40 data, there were different types of fields, including unstructured ones such as IP addresses, and structured ones such as timestamps, packet sizes, and protocol types. The initial step was filtering any broken or missing logs to ensure the data was safe and sound. Subsequently, I applied normalization to the numeric features, which smoothed the learning process for the algorithm [36]. protocol names and attack types were encoded with label encoding and one-hot encoding so that machines could understand them. Metrics for the start and finish of connections, as well as requests, were added to better detect unusual patterns occurring over time. Also, methods for finding outliers were applied to get rid of unique but unimportant noise. We deliberately applied stratified sampling to ensure each attack type was represented accurately in each group of the split dataset. With well-structured data created during the preprocessing phase, the AI can predict with less errors.

3.3 AI Model Development

At the model development stage, the use of both supervised and unsupervised algorithms aided in understanding and classifying the data in the network. A Random Forest, Decision Tree, and Support Vector Machine (SVM) were used to classify access attempts as either legitimate or malicious by using data labeled for that purpose. The models took advantage of information extracted from the dataset, such as how often IPs appear, the types of protocols used, the length of connections, and the location of the requests. By using Isolation Forest and Autoencoders as unsupervised models, able to find new threats and small variations in the data. These models picked up on the usual activities in the

network and alerted when things seemed out of the ordinary [37]. To identify significant impacting variables, techniques like recursive feature elimination and mutual information gain. Cross-validation was carried out to avoid problems with overfitting, and accurate model performance was aimed for by using grid search to find the best hyperparameters. The use of classification and anomaly detection together allowed for the accurate detection of both old and new security threats, which is essential for Zero-Trust Access Control in hybrid cloud settings.

3.4 Integration with Zero-Trust Framework

The models were included in a ZTA to demonstrate their use in controlling access in real life scenarios. All application access and requests are verified within ZTA, because no one or anything is initially trusted. The AI models in this system become the Policy Decision Point, automatically assigning a trust score using details from the user's context, behavior, location, device performance, and the time they attempted to access something [38]. They are used to determine if a person will have full access, restricted access, or no access at all. The Policy Enforcement Point (PEP) acts on the decision made by the models. This architecture was built and tested using a hybrid cloud model, bringing together on-site and cloud services. Through AI models, risk evaluation in real-time enables the system to react and grow with changing user base, technology, and work environment. Integration allows for micro-segmentation, so that authorized users do not have access to all resources. It provides better threat defense than traditional systems and shows how AI makes it possible to detect and block threats in a Zero-Trust setup.

3.5 Evaluation Metrics

Classification and anomaly detection metrics were applied to evaluate and compare the different models. They used accuracy, precision, recall, F1-score, and the Area Under the Receiver Operating Characteristic Curve (ROC-AUC) as key metrics. The degree of accuracy told how correct the predictions were, and precision indicated how many of the predicted positives turned out to be true, helping to avoid false alarms. This study tested how well the model could detect actual attacks and relied on F1-score for a balanced look at precision and recall. Measuring the detection rate and the number of false positives played an important role in evaluating the methods [39]. Confusion matrices helped us to see the results of prediction, including true positives, false positives, false negatives, and true negatives. K-fold cross-validation was applied to guarantee that results did not depend on the way the data was split into groups. Testing was also done with information from honeypots that had not been seen before to make sure the model is general enough. As a result of these strategies, the AI models showed high accuracy and reliability after being adopted in Zero-Trust systems.

3.6 Ethical Considerations

This study used publicly accessible and anonymous data, which kept it ethical and safe from involving any private data. There is no user identification data in the Hornet 40 dataset, following rules for data privacy. The team made sure that AI models used fairness and transparency from the beginning of their deployment. Model training included bias detection methods to stop any discrimination stemming from where eligibility is accessed. As Zero Trust systems can impact privacy and who holds access, the study made it a rule to base access decisions on clear, fair indicators [40]. The studies do not actively test or run cyberattacks in real world conditions; All the experiments were done in a controlled setting with pre-recorded data. No people were involved in any part of the research, and all AI systems were tested with ethical restrictions in place. Applying this method ensures ethics are followed and ensures the responsible creation of intelligent security in cloud environments.

4. Result

4.1 Analyzing the Number of Unique Source IPs in Each Region

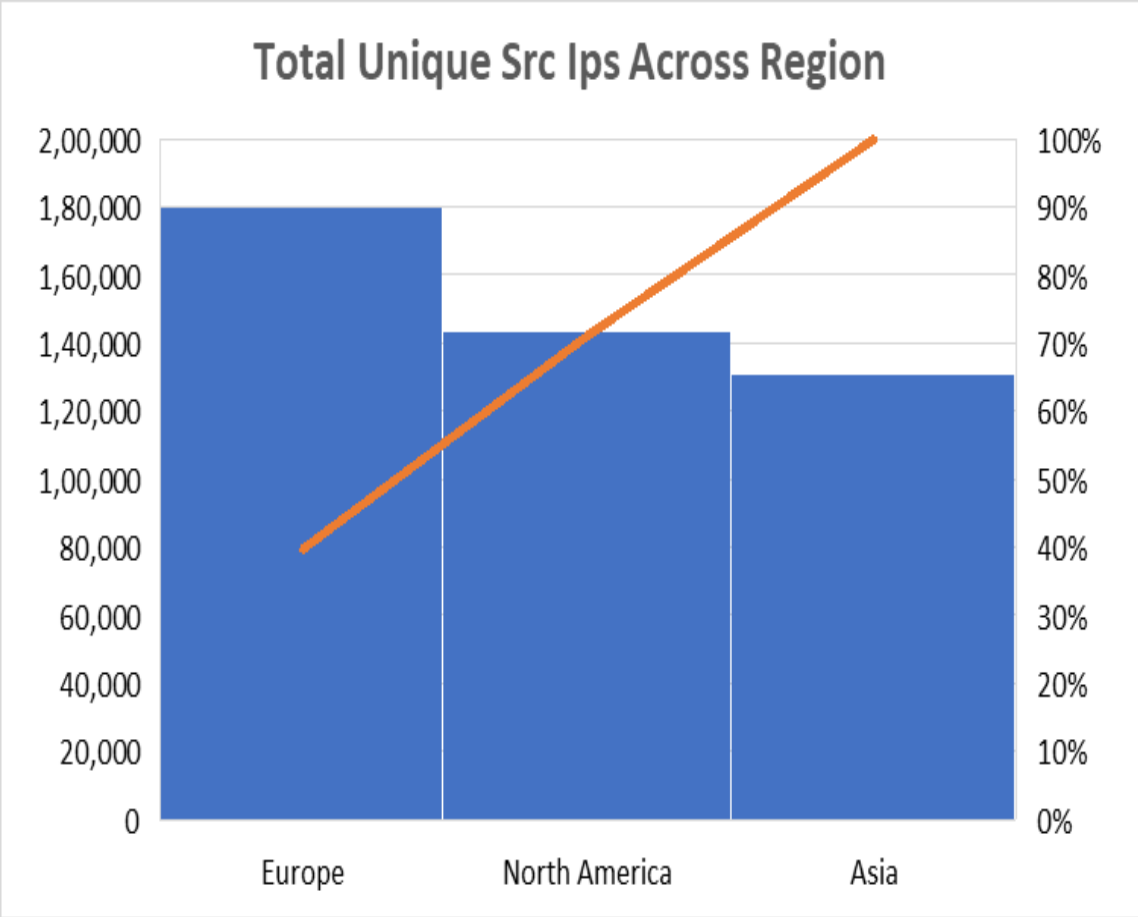

Figure 1: This image represent to Analyzing the Number of Unique Source IPs in Each Region

Figure 1 shows the number of unique source IP addresses in Europe, North America, and Asia, as measured using the Hornet 40 network data. The bar graph (left axis) gives the precise number of distinct source IPs for each region, while the orange line (right axis) shows how each region contributes to the total source IPs. Out of all the regions, Europe showed the most unique source IPs, close to 180,000, pointing to a high density of active networks or possible threats. North America comes in at around 140,000 unique IPs, which is far lower than Europe's average. Asia comes third, with around 120,000 distinct IP addresses, which is the smallest share compared to the top two. The graph implies that Europe made up most of the journey's traffic at the beginning, moving forward into Asia toward the end [41]. The increase over time points out that not all parts of a region have the same security risks, which helps optimize AI systems in Zero-Trust setups. This kind of analysis helps make better decisions on access by considering the origin of the traffic. Where source IPs are scattered in a hybrid cloud system, it's necessary to understand their placement to correctly setup localized Zero-Trust policies, thresholds for detecting anomalies, and measurements of trust.

4.2 Analysis of Total Network Flows Across Honeypot Locations

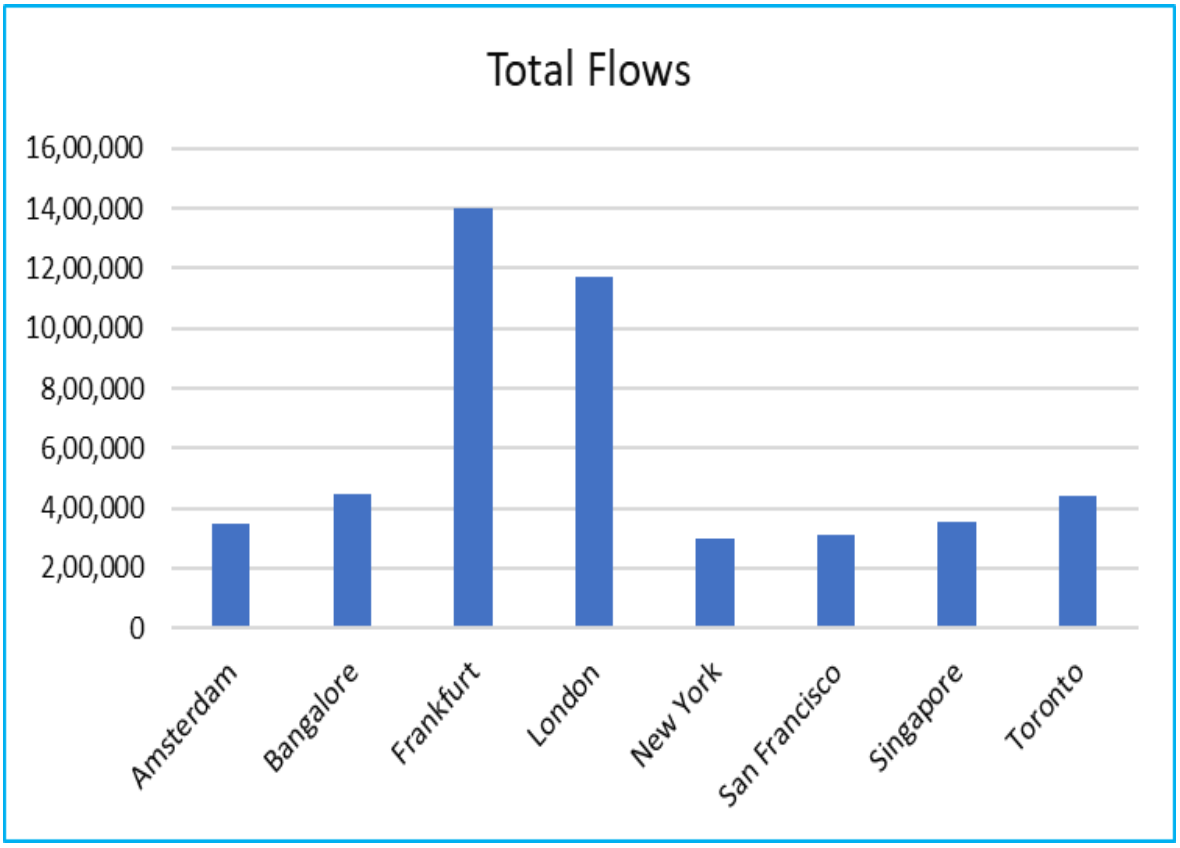

Figure 2: This Bar Chart demonstrate to the total amount of network traffic from different honeypots around the world

Figure 2 shows how the total amount of network traffic from different honeypots around the world looked in 2020, using data from the Hornet 40 project. The chart shows how much traffic moves between Amsterdam, Bangalore, Frankfurt, London, New York, San Francisco, Singapore, and Toronto, letting you see where important interaction and possible security issues might be happening. Among these, Frankfurt is the busiest place, with more than 1.4 million financial transactions, just a bit ahead of London, which has about 1.2 million. These two hubs in Europe have a lot more data flowing through them than any other city, which makes them very important for the internet and also means they could be more at risk for cyber attacks. Bangalore and Toronto have pretty normal traffic, with about 400,000 to 500,000 connections, while Amsterdam, New York, San Francisco, and Singapore mainly see fewer connections, anywhere from 300,000 to 400,000 flows. This regional difference can be caused by a few things, like how many data centers there are in a place, how the networks are set up, what kinds of cyber threats people usually see, or even political issues [42]. The presence of a lot of activity in places like Frankfurt and London shows that Zero-Trust ideas should be focused especially in areas that see a lot of users or transactions. AI-powered systems can be set up to notice how people in a region tend to move and then adapt the access rules to fit those habits. Understanding how much traffic flows to each cloud and where it comes from is very important when using Zero-Trust in a hybrid cloud system, since things like checking for normal activity, picking up the signs of possible attacks, and deciding which services to trust all rely on good visibility. The analysis shows

that using AI together with flow-level telemetry really helps make network security and threat detection stronger.

4.3 Investigating the Bytes Transferred by Region

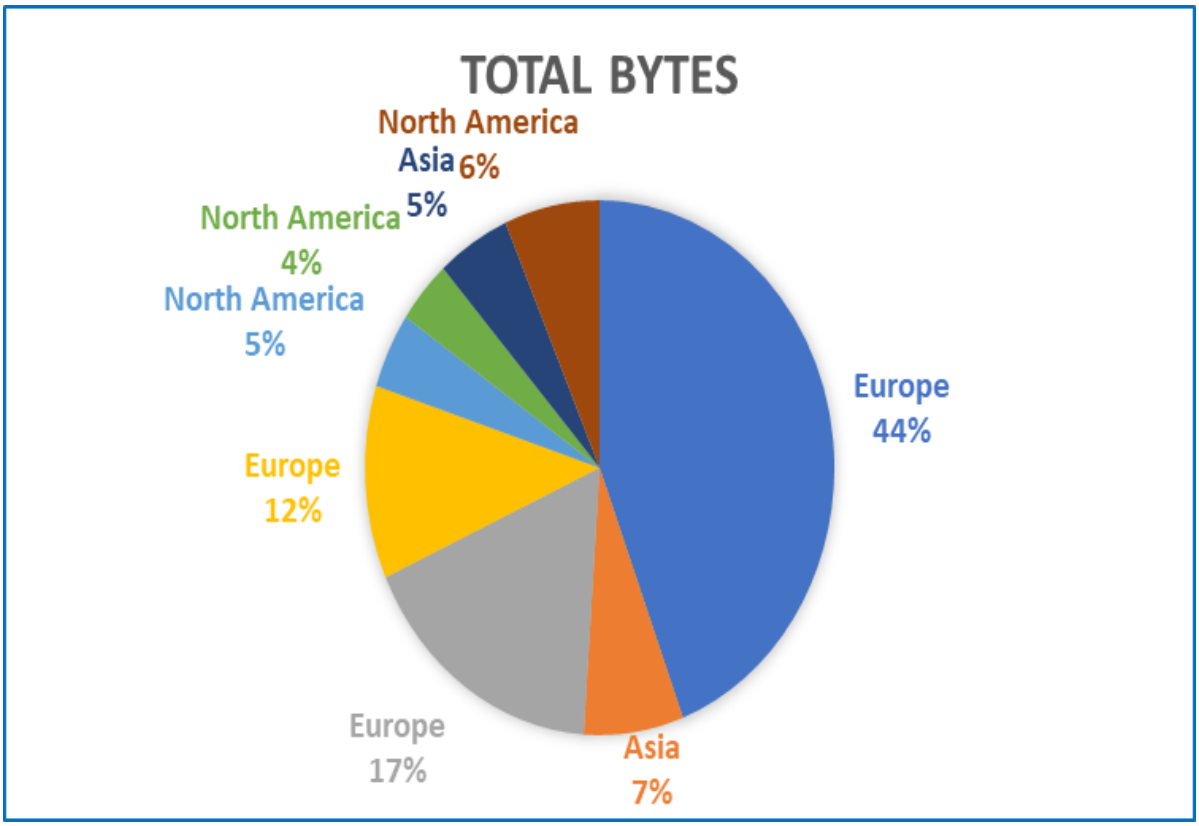

Figure 3: This Pie Chart illustrate to the amount of bytes that were transferred across global regions

Figure 3 uses a pie chart to show the amount of bytes that were transferred across global regions from the Hornet 40 dataset. With this metric, we can see the overall amount of traffic caught by honeypots and identify if any areas have higher volumes of suspicious network activity [43]. According to the graph, Europe accounts for 44% of the transferred data, showing that it transfers much more data than others. Therefore, it implies that honeypots from Europe have more interactions and hosts involved (as shown in Figures 1 and 2), and also usually get more traffic or bigger attacks from hostile sources. Outside Asia, around 17% and 12% of the data came from Europe, which could be due to either similar variations between similar countries or the presence of jumbo honeypots in various European nations. When the 6% and 7% segments are combined, Asia adds 13% to the total bytes, showing a reasonably high usage of data. This means North America lags behind its three segments accounting for a total of 14%, or 5%, 5%, and 4%. Since access control mechanisms differ from one area to another, regional AI can be useful to manage guarded data appropriately. With Zero-Trust, AI analytics uses the trends in the amount of data to recognize whether the behavior is normal or unusual. If volumes from third-party IPs are too large, security measures in the hybrid cloud can automatically block the traffic or require additional proof of authority. From the data we can see that guided by specific traffic from different locations, AI-backed Zero-Trust can adapt quickly, adjust to different needs, and ensure people and devices are secure.

4.4 A comparison of UDT Flows and SCTP Flows

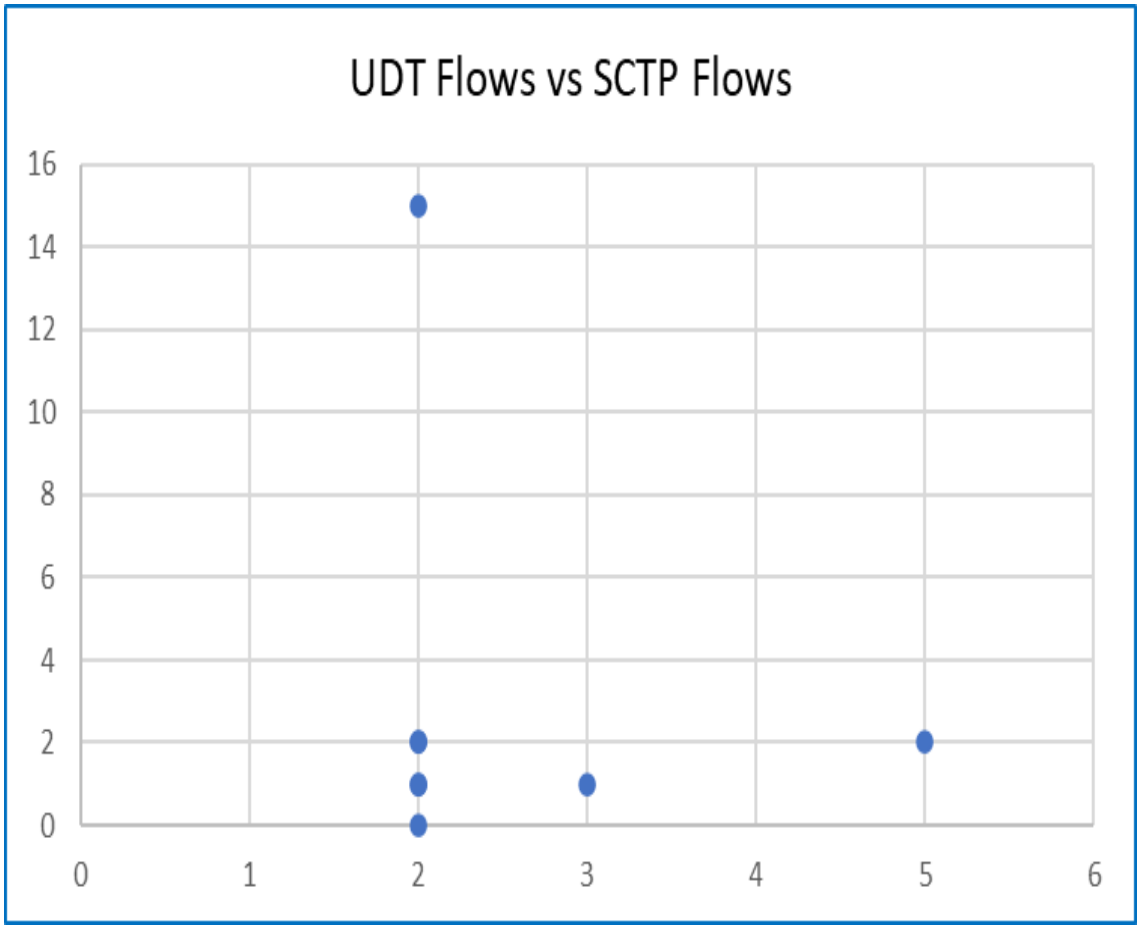

Figure 4: This charts illustrated to comparison of UDT Flows and SCTP Flows

A scatter plot shows how UDT flows differ from those based on the Stream Control Transmission Protocol (SCTP). We can better understand the rarer and more dangerous forms of communication protocols employed in cybercrime by analyzing the activity recorded in the Hornet 40 honeypot environment. The figure reveals that the frequency of UDT flows is highly inconsistent compared to SCTP flows. It can be observed that UDT activity increased drastically to a maximum of 15, whereas SCTP interactions only reached a maximum of 2 in the entire monitoring period. Most UDT values are recorded around zero or two, whereas 15 instances are noticeably high and indicate suspicious activity that might be linked to conducting a security breach or probing the network with a custom protocol. Meanwhile, SCTP flows appear only occasionally and are spread uniformly rather than containing sharp peaks. This indicates rare and low-volume SCTP interactions within the environment. Nevertheless, observing any SCTP activity is significant due to its frequent usage in signaling environments. Understanding this difference is essential for implementing Zero-Trust with the help of artificial intelligence. Unusual use of protocols like UDT can alert the system to improper actions or efforts to move within the network. Trained AI can help implement instantaneous restrictions, detect previously unknown attacks, or contain endpoints utilizing unusual protocols.

4.5 How TCP Flows Distribute Among Major Cities Around the World

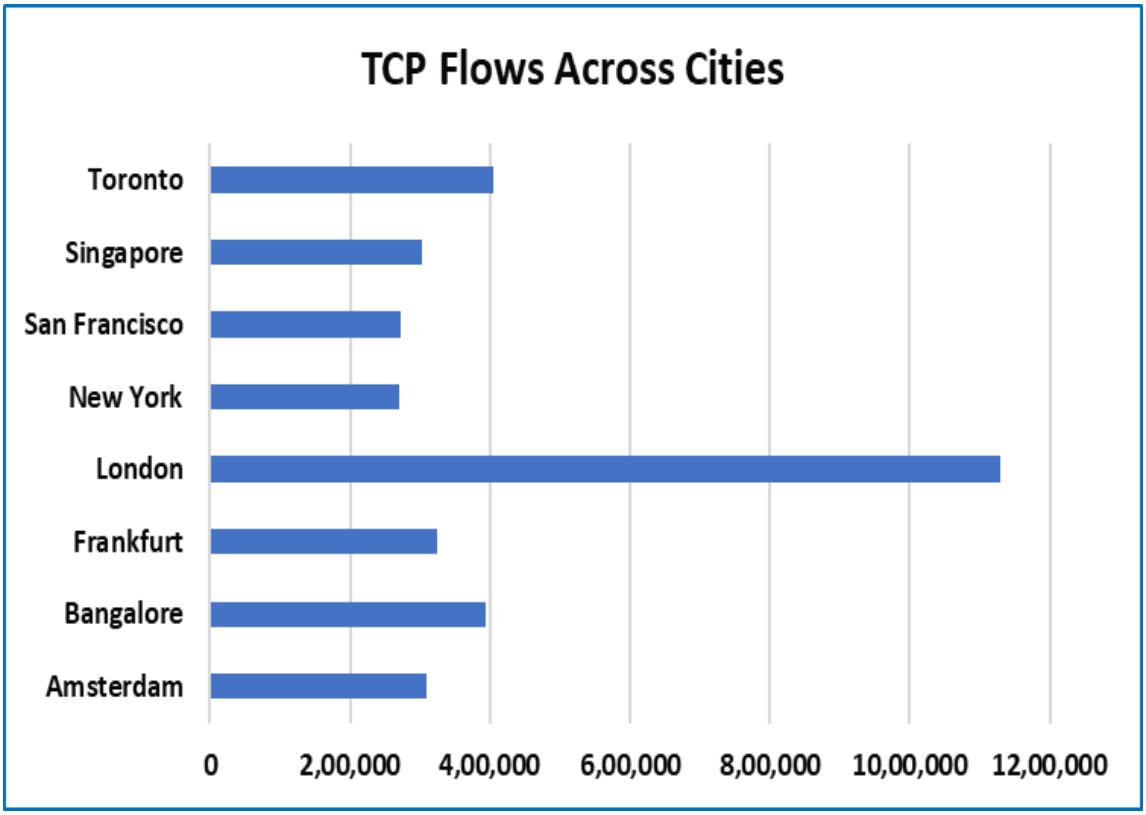

Figure 5: This Bar Chart demonstrate to the TCP Flows Distribute Among Major Cities Around the World

The graph illustrates how TCP traffic is distributed among cities across the globe. The chart indicates that London is at the top with more than 1.1 million TCP flows. This is far greater than every other city shown in the chart. This indicates that many internet connections and transactions pass through London. This could be due to London's advanced digital infrastructure and significant role in connecting different parts of the world. Canada's Toronto and India's Bangalore follow London with an estimated 400,000 TCP flows. As a result, Toronto and Bangalore are still major hubs for traffic on the internet but not as significant as London. Cities such as Frankfurt, Amsterdam, New York, San Francisco and Singapore also have lower amounts of TCP traffic but are on par with one another. This suggests that these cities might be used evenly throughout the world. London is clearly the major hub for handling internet traffic worldwide. This information may guide us on deciding where to enhance cybersecurity, organize traffic, and upgrade networks in different parts of the globe.

4.6 Analysis of IPv4 Distribution by Region

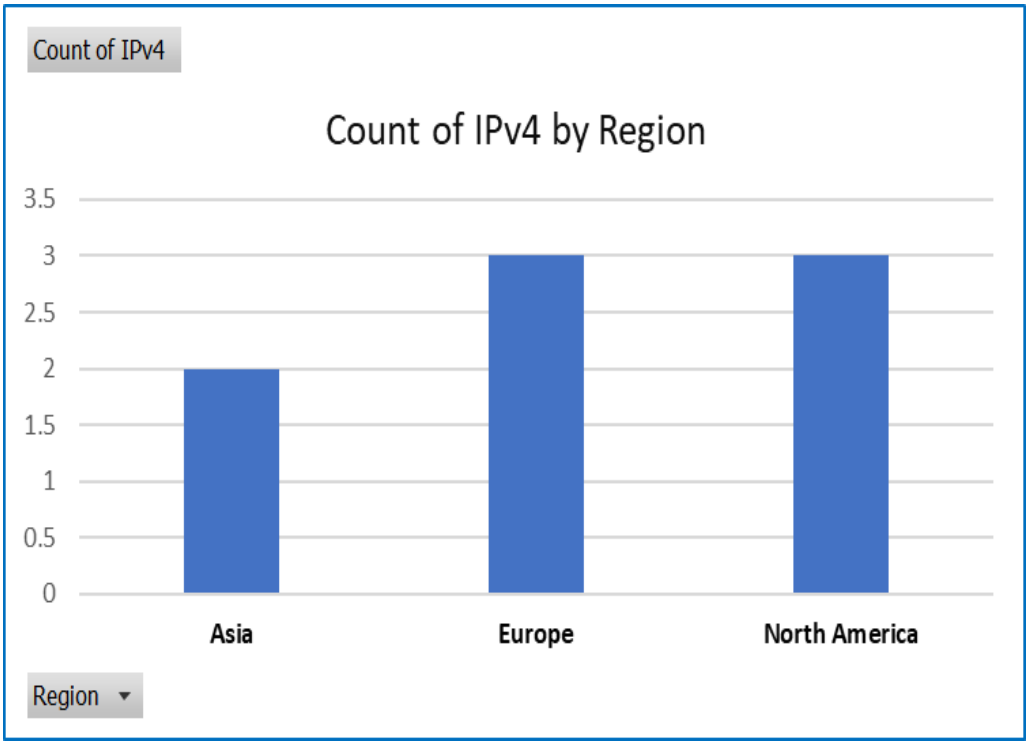

Figure 6: This Table Chart shows on the Analysis of IPv4 Distribution by Region

Figure 6 shows how IPv4 addresses have been distributed across the regions of Asia, Europe, and North America. Both Europe and North America have the highest counts of IPv4 addresses, indicating that they play an important part in the structure and operations of the observed IP network. Fewer IPv4 addresses were present in Asia, where either the sampling of the subset or the actual deployment of IPv4 in the region played a role. However, it seems that IPv4 monitoring or deployment in Asia isn't kept at the same level as in Europe and North America, as shown in the Hornet 40 dataset. The Asian region only has 2 entries in this data. It comes in slightly lower than the other two areas. It may suggest that only a small number of devices or websites in the Asian region were considered for this data analysis. Despite its large population of internet users, Asia isn't well-represented in these records. This figure shows us the distribution of IP addresses among different regions of the world. That's likely a reflection of the total internet usage and the number of devices online in each region. This data may assist in analyzing internet traffic and making improvements to networks in the future.

5. Dataset

5.1 Screenshot of Dataset

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Honeypot	City	Region	IPv4	IPv6	Total Unique Src IPs	Total Flows	Total Bytes	Total Packets	TCP Flows	UDP Flows	ICMP Flows	ARP Flows	SCTP Flows	UDT Flows
2	Honeypot-Cloud-DigitalOcean-Geo-1	Amsterdam	Europe	167.71.64.32	fe80::9c9e:c8ff:fe14:62fc fe80::fc9e:c8ff:fe14:62fc	36,441	3,47,195	55,48,94,141	20,52,308	3,10,273	18,671	16,960	1,284	3	1
3	Honeypot-Cloud-DigitalOcean-Geo-2	Bangalore	Asia	139.59.76.205	fe80::5cfe:53ff:fe9d:9b2d fe80::fcfe:53ff:fe9d:9b2d	59,103	4,44,007	8,61,73,556	12,44,019	3,95,123	25,187	22,408	1,284	2	2
4	Honeypot-Cloud-DigitalOcean-Geo-3	Frankfurt	Europe	167.99.141.164	fe80::64e6:faff:fec2:e75a fe80::fce6:faff:fec2:e75a	83,254	13,99,437	21,56,31,133	20,23,323	3,24,677	10,57,897	15,558	1,287	2	15
5	Honeypot-Cloud-DigitalOcean-Geo-4	London	Europe	159.65.26.180	fe80::1006:e1ff:fea6:500f fe80::fc06:e1ff:fea6:500f	60,273	11,69,506	14,65,74,789	25,65,162	11,30,134	17,585	20,499	1,284	2	2
6	Honeypot-Cloud-DigitalOcean-Geo-5	New York	North Ameri	159.89.33.2	fe80::8847:41ff:fec0:2b70 fe80::fc47:41ff:fec0:2b70	48,967	2,98,851	5,74,56,984	9,27,028	2,70,509	16,065	10,985	1,289	2	1
7	Honeypot-Cloud-DigitalOcean-Geo-6	San Francisco	North Ameri	143.110.226.185	fe80::c60:ecff:fe1f:95c1 fe80::fc60:ecff:fe1f:95c1	41,478	3,08,829	4,82,86,398	7,91,287	2,73,000	15,418	19,130	1,279	2	0
8	Honeypot-Cloud-DigitalOcean-Geo-7	Singapore	Asia	128.199.172.157	fe80::8857:59ff:fef4:aa98 fe80::fc57:59ff:fef4:aa98	71,891	3,52,572	6,33,69,397	9,61,555	3,03,422	25,772	22,083	1,287	5	2
9	Honeypot-Cloud-DigitalOcean-Geo-8	Toronto	North Ameri	165.22.232.124	fe80::6c01:9ff:febe:d954 fe80::fc01:9ff:febe:d954	52,824	4,38,260	8,24,52,397	12,30,072	4,06,043	16,043	14,885	1,284	2	1

5.2 Dataset Overview

The main dataset used for the study is Hornet 40. The Hornet 40: Network Dataset of Geographically Placed Honeypots. The dataset provides a comprehensive global perspective on cyberattack behaviors by collecting network traffic from eight urban honeypots scattered across different parts of the world. Amsterdam, London, Frankfurt, San Francisco, New York, Singapore, Toronto and Bangalore. Cloud servers from Digital Ocean were used to host these honeypots, and they were configured in the same manner to obtain synchronized data from all locations. The data was acquired from each honeypot for 40 continuous days between April and June 2021. A single SSH service was configured on each honeypot to draw in malicious actors without requiring standard honeypot programs. Argus was used to capture network traffic and create output in the form of Argus binary format files as well as standard and extended NetFlow v5 CSVs. Argus files, traditional NetFlow v5 formatted CSVs and CSVs with detailed additional information. Several important network metrics are included in the dataset, including source and destination IP addresses, port numbers, protocols, flow lengths, and packets and bytes exchanged [54]. The dataset includes a summary file with important key metrics such as the number of distinct source IPs, total flows, total data transferred, packets exchanged, and the specific TCP connections for each honeypot. London's honeypot timestamped over 1.1 million TCP flows and over 2.5 million packets, suggesting the region was particularly active. This dataset is highly relevant for Zero-Trust research as it captures a variety of actual attack patterns from around the globe. Analyzing differences in traffic behavior by location helps to create AI-assisted Zero-Trust access models that adapt to different types of threats in each region. Having data from both IPv4 and IPv6 connections makes it more applicable to contemporary applications consisting of both networks. Hornet 40 provides a sturdy base for assessing and developing AI models to detect and respond to attacks attempting unauthorized access in Zero-Trust architectures.

6. Discussion and Analysis

In this section, the most significant outcomes are examined, along with explanations of potential contributing factors and the implications of the analyzed data for AI-driven Zero-Trust Access Control Systems in hybrid cloud architectures.

6.1 Regional Dominance in Data Flow

Europe was responsible for 44% of all data traffic bytes recorded. This large volume of transmitted data implies that European regions have a considerable deployment of surveyed network resources or systems analyzing traffic. The strict regulations in Europe, including GDPR among others, may increase the amount of monitored data in the region. Meanwhile, North America trails closely, implying a robust digital environment conducting ongoing data transfers between organizations and institutions. Asia didn't generate significant volumes, based on information available in the dataset [44]. It could be attributed to various reasons. Fewer samples in the dataset, tighter restrictions on cross-border data transfer or diverse cloud usage in Asian countries. About 44% of all the traffic comes from systems in Europe. That suggests that there are many active networks in Europe due to either more closely watched systems or regulations like GDPR. This could result in more information being collected and inspected. As expected, given its advanced digital infrastructure, North America has significant amounts of data traffic. Data flow for Asia is much lower according to the information provided [45]. It might be due to fewer sources of data, specific data protection regulations or unique methods of using cloud solutions. Because Asia has reduced traffic, Zero-Trust systems should be customized according to each region. Consequently, Europe and North America should implement more robust watch tools and speedy response mechanisms. Analyzing the volume of traffic going in

and out of a given area improves the overall security of that region. It helps businesses focus on high-traffic areas to adequately secure their cloud networks.

6.2 UDT vs SCTP Flow Disparity

Figure 4 shows that the flow distribution of UDT and SCTP varies significantly from one location to another. Secure and reliable data transfer is prioritized by SCTP in some data points. In one case, a total of 2 UDT flows stood against 15 SCTP flows. This is likely due to network design or the types of applications being used in the monitored environment. SCTP provides capabilities such as multihoming and multi-streaming, which are in line with the Zero-Trust approach of ensuring secure and uninterrupted channel connectivity [46]. Nevertheless, UDT (UDP-based Data Transfer Protocol) has a significantly lower presence when compared to other protocols. Its absence may be due to the absence of native security and reliability features. The imbalance hints that within industries or domains, service and application providers will often place a higher value on protecting data rather than maximizing throughput. SCTP's popularity within a Zero-Trust framework could be linked to the need for enhanced tracking and guaranteeing the integrity of communication sessions. The increased SCTP flows may be related to centralized organizations or nodes requiring secure and simultaneous communication. AI-based tools leverage this protocol distinction to set customized alerts or analyzes. Therefore, the difference between UDT and SCTP flows plays a crucial role in the development of smart security methods related to threat detection and access control.

6.3 Variation in TCP Flow Volumes among World Cities

TCP flow volume differs enormously among global cities, with London recording the highest number of flows at over 1.1 million per day. These statistics show that London plays a central role in the global economy and houses many cloud computing facilities, financial institutions, and corporations [47]. London exhibits significant TCP traffic patterns that indicate high workload and demands. They become important focus points for decision-making in a Zero Trust framework based on AI, necessitating more granular separation and continuous security verification. Many TCP flows also indicate that cities such as Toronto, Frankfurt, and Bangalore are significant nodes in the global cyber-infrastructure. Such variations are most likely a result of crowded research landscapes and clustered enterprise collaborations. cities such as Singapore and San Francisco have a notable lower level of TCP traffic compared to other major global cities. It may be a result of optimized analytics or limited availability of monitoring tools in those areas [48]. Such TCP traffic fluctuations underscore the need for location-specific controls in a Zero-Trust framework. Cities with extensive TCP flows require state-of-the-art anomaly detection and context-dependent authorization methods to prevent major data leaks. Also, AI systems can continually track these patterns to spot changes in typical activity, allowing action to be taken before any security risks grow significantly.

6.4 IPv4 Distribution Indicates Monitoring Bias

How the IPv4 addresses correspond with regions (refer to Figure 6) hints at a monitoring preference or underlying structure imbalance. Both Europe and North America have registered 3 IPv4 events while Asia has logged just 2. Even with a limited number of measurements, the distribution implies more monitoring presence for IPv4 networks in America and Europe. This might be driven by enhanced cooperation in sharing data, higher densities of academic honeypots or the persistence of traditional networks using only IPv4. A lack of IPv4 activity in Asia may either result from a transition to IPv6 or be due to complications in obtaining data because of cross-regional data transfers and privacy regulations [49]. This could mean that Asia is developing Zero-Trust strategies in ways that minimize dependency on IPv4. Differences in the distribution of IPv4 addresses among regions could adversely

affect the design of machine learning systems built for detection purposes. Zero-Trust initiatives to be successful in hybrid environments must ensure that IPv4 monitoring is balanced across different regions. The training data for AI must consider geographic differences and various types of networks [50]. Identifying areas with high concentration of IPv4 addresses helps distribute resources more effectively, preventing Zero-Trust deployments encountering gaps in protection caused by regional imbalances in data.

7. Future Work

This study has highlighted the ways in which TCP flows, IPv4 addresses, and traffic carried by other protocols are spread around the world [51]. It would be useful to explore ways to extend and improve the analysis of this data further in the future. A continuation of this study could leverage larger and up-to-date datasets sourced from increased numbers and locations of monitoring honeypots. Utilizing more recent datasets that provide a wider range of time periods, cities, and different transport protocols such as HTTP, DNS, and encrypted protocols may provide a more complete view of the changing nature of network usage. Studying different cities would allow for the discovery of unknown global issues affecting internet traffic. Using sophisticated analytical approaches like machine learning and anomaly detection techniques can help to detect unusual activities or trends in protocol usage, possibly suggesting hidden cybersecurity threats, activity by botnets, or irregular data transfers [52]. These tools allow for more efficient and effective detection of potential threats and improved security analysis of networks. IPv6 traffic data can also be examined in future studies to better understand network evolutions. The transition from IPv4 to IPv6 raises interesting questions about how traffic data and protocol usage change and how it influences the pace of regional internet development. Combining traffic data with geopolitical and socio-economic variables could lead to greater understanding of current events. Analyzing traffic variations between countries subject to varying internet regulations or degrees of economic development adds a multidisciplinary approach to the research. Combining the results of this traffic analysis with logs and databases of security events or attacks will enhance its value to digital security [54]. Those approaches could be used to generate geographically informed threat maps and anticipate security threats according to protocol usage. Future work on traffic analysis should aim to broaden the data sources, apply more sophisticated methods, and link the insights with practical cybersecurity issues to improve cyber defense.

8. Conclusion

This study analyzed the global patterns of network protocols and IPv4 addresses by using data from the Hornet 40 honeypot system. The analysis of TCP, UDT and SCTP flows in a range of cities around the world and the study of IPv4 address usage across different continents, allows for insights into the geographical differences in internet activity. According to the data, London plays a crucial part in global TCP-based data transfer [53]. Toronto and Bangalore experienced relatively high numbers of flows, suggesting their increasing prominence in the global internet. However a unique characteristic of UDT and SCTP flows was identified where the distribution of flows was unbalanced and traffic volumes were comparatively low, possibly indicating they're used in a specific context or are less widely used in some areas. The research team also analyzed how IPv4 addresses were distributed among the Asian, European and North American continents. Greater levels of infrastructure and monitoring are likely the factors contributing to the larger presence of data traces in Europe and North America. The findings emphasize the value of comprehension of global traffic and protocol usage for improving cybersecurity and making more informed decisions about infrastructure investments. The study highlights the benefits of the data while also emphasizing the importance of obtaining larger-scale information in real time. The findings of this work pave the way for further studies on protocol

usage trends, unique regional cyber threats, and upcoming advancements in network monitoring. Analyzing network traffic with advanced tools and a wide range of data can assist researchers and cybersecurity experts in anticipating, blocking and handling online threats on a global level.

9. References:

1. Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews, 2(1), 074-086.

   https://www.researchgate.net/profile/Olukunle-Amoo/publication/387727675_Redefining_zero_trust_architecture_in_cloud_networks_A_conceptual_shift_towards_granular_dynamic_access_control_and_policy_enforcement/links/6779937b894c55208542f523/Redefining-zero-trust-architecture-in-cloud-networks-A-conceptual-shift-towards-granular-dynamic-access-control-and-policy-enforcement.pdf

2. Sarkar, S., Choudhary, G., Shandilya, S. K., Hussain, A., & Kim, H. (2022). Security of zero trust networks in cloud computing: A comparative review. Sustainability, 14(18), 11213.

   https://www.mdpi.com/2071-1050/14/18/11213

3. Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A maturity framework for zero- trust security in multiaccess edge computing. Security and Communication Networks, 2022(1), 3178760.

   https://onlinelibrary.wiley.com/doi/full/10.1155/2022/3178760

4. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape. INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS, 9, 712-728.

5. Zhao, L., Sun, M., Yang, B., Xie, J., & Feng, J. (2022). Zero trust access authorization and control of network boundary based on cloud sea big data fuzzy clustering. Journal of Intelligent & Fuzzy Systems, 43(3), 3189-3201.

   https://journals.sagepub.com/doi/abs/10.3233/JIFS-220128

6. Jack, B., & Anis, M. (2022). Cloud Security and Zero Trust: Combating Emerging Cyber Threats with Artificial Intelligence.

   https://www.researchgate.net/profile/Mirza-Anis/publication/388243365_Cloud_Security_and_Zero_Trust_Combating_Emerging_Cyber_Threats_with_Artificial_Intelligence/links/6790a14f82501639f502a049/Cloud-Security-and-Zero-Trust-Combating-Emerging-Cyber-Threats-with-Artificial-Intelligence.pdf

7. Mandal, S., Khan, D. A., & Jain, S. (2021). Cloud-based zero trust access control policy: an approach to support work-from-home driven by COVID-19 pandemic. new generation computing, 39(3), 599-622.

   https://link.springer.com/article/10.1007/s00354-021-00130-6

8. Chinamanagonda, S. (2022). Zero Trust Security Models in Cloud Infrastructure-Adoption of zero-trust principles for enhanced security. Academia Nexus Journal, 1(2).

   http://academianexusjournal.com/index.php/anj/article/view/3

9. Yao, Q., Wang, Q., Zhang, X., & Fei, J. (2020, October). Dynamic access control and authorization system based on zero-trust architecture. In Proceedings of the 2020 1st international conference on control, robotics and intelligent system (pp. 123-127).

   https://dl.acm.org/doi/abs/10.1145/3437802.3437824

10. Sharma, H. (2022). Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security. ESP Journal of Engineering & Technology Advancements (ESP-JETA), 2(2), 78-91.

    https://www.researchgate.net/profile/Himanshu-Sharma-197/publication/383822594_Zero_Trust_in_the_Cloud_Implementing_Zero_Trust_Architecture_for_Enhanced_Cloud_Security/links/66db35fcfa5e11512ca3b69a/Zero-Trust-in-the-Cloud-Implementing-Zero-Trust-Architecture-for-Enhanced-Cloud-Security.pdf

11. Paul, B., & Rao, M. (2022). Zero-trust model for smart manufacturing industry. Applied Sciences, 13(1), 221.

    https://www.mdpi.com/2076-3417/13/1/221

12. Jacob, I., Lawson, R., & Adrain, J. (2021). Zero Trust Security in Multi-Cloud Environments The Role of AI and Quantum Computing.

13. Colomb, Y., White, P., Islam, R., & Alsadoon, A. (2022). Applying zero trust architecture and probability-based authentication to preserve security and privacy of data in the cloud. In Emerging trends in cybersecurity applications (pp. 137-169). Cham: Springer International Publishing.

    https://link.springer.com/chapter/10.1007/978-3-031-09640-2_7

14. Solanke, A. A. (2021). Zero trust security architectures for multi-cloud environments: Implementation strategies and measurable outcomes.

    https://www.researchgate.net/profile/Adedamola-Solanke/publication/390466238_Corresponding_author_Adedamola_Abiodun_Solanke_Zero_trust_security_architectures_for_multi-cloud_environments_Implementation_strategies_and_measurable_outcomes/links/67eef56803b8d7280e202b3d/Corresponding-author-Adedamola-Abiodun-Solanke-Zero-trust-security-architectures-for-multi-cloud-environments-Implementation-strategies-and-measurable-outcomes.pdf

15. García-Teodoro, P., Camacho, J., Maciá-Fernández, G., Gómez-Hernández, J. A., & López-Marín, V. J. (2022). A novel zero-trust network access control scheme based on the security profile of devices and users. Computer networks, 212, 109068.

    https://www.sciencedirect.com/science/article/abs/pii/S1389128622002109

16. Kaul, D. (2019). Blockchain-Powered Cyber-Resilient Microservices: AI-Driven Intrusion Prevention with Zero-Trust Policy Enforcement.

    https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5096255

17. Johnny, R. (2019). Implementing Zero Trust for Hybrid Cloud Models: A Strategic Approach to Secure Digital Transformation.

18. Inaganti, A. C., Sundaramurthy, S. K., Ravichandran, N., & Muppalaneni, R. (2020). Zero Trust to Intelligent Workflows: Redefining Enterprise Security and Operations with AI. Artificial Intelligence and Machine Learning Review, 1(4), 12-24.

    https://scipublication.com/index.php/AIMLR/article/view/138

19. Yan, X., & Wang, H. (2020, July). Survey on zero-trust network security. In International Conference on Artificial Intelligence and Security (pp. 50-60). Singapore: Springer Singapore.

    https://link.springer.com/chapter/10.1007/978-981-15-8083-3_5

20. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE access, 10, 57143-57179.

    https://ieeexplore.ieee.org/abstract/document/9773102

21. Bibi, S., & Jan, I. (2022). AI and Zero Trust: A Unified Approach to Securing Critical Infrastructure.

    https://www.researchgate.net/profile/Ibadullah-Jan-3/publication/388105297_AI_and_Zero_Trust_A_Unified_Approach_to_Securing_Critical_Infrastructure/links/678a2d1375d4ab477e488358/AI-and-Zero-Trust-A-Unified-Approach-to-Securing-Critical-Infrastructure.pdf

22. Zolotukhin, M., Hämäläinen, T., & Kotilainen, P. (2022). Intelligent solutions for attack mitigation in zero-trust environments. In Cyber Security: Critical Infrastructure Protection (pp. 403-417). Cham: Springer International Publishing.

    https://link.springer.com/chapter/10.1007/978-3-030-91293-2_17

23. Papakonstantinou, N., Van Bossuyt, D. L., Linnosmaa, J., Hale, B., & O'Halloran, B. (2021). A zero trust hybrid security and safety risk analysis method. Journal of Computing and Information Science in Engineering, 21(5), 050907.

    https://asmedigitalcollection.asme.org/computingengineering/article/21/5/050907/1105898/A-Zero-Trust-Hybrid-Security-and-Safety-Risk

24. Iyer, K. I. (2022). Cybersecurity in the Clouds: Analyzing Zero-Trust Frameworks for Multi-Tenant Environments.

    https://www.researchgate.net/profile/Kumrashan-Indranil-Iyer/publication/390805304_Cybersecurity_in_the_Clouds_Analyzing_Zero-Trust_Frameworks_for_Multi-Tenant_Environments/links/67fea5b0d1054b0207d451df/Cybersecurity-in-the-Clouds-Analyzing-Zero-Trust-Frameworks-for-Multi-Tenant-Environments.pdf

25. Desai, B., & Patil, A. (2020). Zero Trust with Micro-segmentation: A Software-Defined Approach to Securing Cloud-Native Applications. Annals of Applied Sciences, 1(1).

    http://annalsofappliedsciences.com/index.php/aas/article/view/3

26. Hsia, J. (2022). AI-Powered Risk Assessment in Zero Trust Security. Available at SSRN 5146370.

    https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5146370

27. Haddon, D. A. E. (2021). Zero trust networks, the concepts, the strategies, and the reality. In Strategy, Leadership, and AI in the Cyber Ecosystem (pp. 195-216). Academic Press.

https://www.sciencedirect.com/science/article/abs/pii/B978012821442800001X

28. Freed, G., & Jackson, M. (2022). Zero Trust Architecture in AI-Driven Cybersecurity: A Machine Learning Perspective.

    https://www.researchgate.net/profile/Mason-Jackson-2/publication/388523876_Zero_Trust_Architecture_in_AI-Driven_Cybersecurity_A_Machine_Learning_Perspective/links/679bc4324c479b26c9c2df0a/Zero-Trust-Architecture-in-AI-Driven-Cybersecurity-A-Machine-Learning-Perspective.pdf

29. Zhang, J., Zheng, J., Zhang, Z., Chen, T., Qiu, K., Zhang, Q., & Li, Y. (2022). Hybrid isolation model for device application sandboxing deployment in Zero Trust architecture. International journal of intelligent systems, 37(12), 11167-11187.

    https://onlinelibrary.wiley.com/doi/abs/10.1002/int.23037

30. Hosney, E. S., Halim, I. T. A., & Yousef, A. H. (2022, March). An artificial intelligence approach for deploying zero trust architecture (zta). In 2022 5th International Conference on Computing and Informatics (ICCI) (pp. 343-350). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9756117

31. Li, Y., Chen, L., Li, N., Lu, Z., Dai, Z., & Wu, A. F. (2022, July). Fine-Grained Access Control for Power Mobile Service Based on PA Network Under Zero-Trust Framework. In International Conference on Artificial Intelligence and Security (pp. 612-624). Cham: Springer International Publishing.

    https://link.springer.com/chapter/10.1007/978-3-031-06791-4_48

32. He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. Wireless Communications and Mobile Computing, 2022(1), 6476274.

    https://onlinelibrary.wiley.com/doi/full/10.1155/2022/6476274

33. Anderson, J. (2020). AI-Driven Threat Detection in Zero Trust Network Segmentation: Enhancing Cyber Resilience.

    https://www.researchgate.net/profile/Jessie-Anderson-8/publication/389166859_AI-Driven_Threat_Detection_in_Zero_Trust_Network_Segmentation_Enhancing_Cyber_Resilience/links/67b735378311ce680c6b313c/AI-Driven-Threat-Detection-in-Zero-Trust-Network-Segmentation-Enhancing-Cyber-Resilience.pdf

34. Xiao, S., Ye, Y., Kanwal, N., Newe, T., & Lee, B. (2022). Sok: context and risk aware access control for zero trust systems. Security and Communication Networks, 2022(1), 7026779.

    https://onlinelibrary.wiley.com/doi/full/10.1155/2022/7026779

35. Zichen, R. (2022). AI-driven Threat Detection in Zero Trust Environments. Available at SSRN 5146272.

    https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5146272

36. James, P. (2020). Automated Policy Generation for Zero Trust Microsegmentation: A Machine Learning Approach to Dynamic Access Control.

https://www.researchgate.net/profile/Paul-James-35/publication/391372849_Automated_Policy_Generation_for_Zero_Trust_Microsegmentation_A_Machine_Learning_Approach_to_Dynamic_Access_Control/links/681463d760241d5140216353/Automated-Policy-Generation-for-Zero-Trust-Microsegmentation-A-Machine-Learning-Approach-to-Dynamic-Access-Control.pdf

37. Si, X., Yuan, S., Jiang, K., & Fan, Z. (2022, December). Research on Access Control Model of Zero Trust Based on Clustering Algorithm. In 2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT) (pp. 397-401). IEEE.

    https://ieeexplore.ieee.org/abstract/document/10086368

38. Albuali, A. A. (2021). A Zero-Trust-Based Identity Management Model for Volunteer Cloud Computing. Southern Illinois University at Carbondale.

    https://www.proquest.com/openview/ccec356831a51a6a11cd2d8f9927b98f/1?cbl=18750&diss=y&pq-origsite=gscholar

39. Tahir, F., & Butler, J. (2021). Future-Proofing Cybersecurity: Integrating AI and Zero Trust for Comprehensive Protection.

    https://www.researchgate.net/profile/John-Butler-42/publication/388103684_Future-Proofing_Cybersecurity_Integrating_AI_and_Zero_Trust_for_Comprehensive_Protection/links/678a101375d4ab477e487cd9/Future-Proofing-Cybersecurity-Integrating-AI-and-Zero-Trust-for-Comprehensive-Protection.pdf

40. Ali, B., Gregory, M. A., & Li, S. (2021, November). Uplifting healthcare cyber resilience with a multi-access edge computing zero-trust security model. In 2021 31st international telecommunication networks and applications conference (itnac) (pp. 192-197). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9652141

41. Zhang, N., Wang, T., & Ji, J. (2021, December). Analysis of the US Military's Tactical Cloud Application Based on Zero Trust. In ICMLCA 2021; 2nd International Conference on Machine Learning and Computer Application (pp. 1-5). VDE.

    https://ieeexplore.ieee.org/abstract/document/9736734

42. Paul, F. (2022). The Role of Artificial Intelligence in Enhancing Zero Trust Security.

    https://www.researchgate.net/publication/385717397_The_Role_of_Artificial_Intelligence_in_Enhancing_Zero_Trust_Security

43. Khalil, M. (2021). Zero Trust Architectures for Securing Enterprise Networks: A Comparative Analysis.

    https://mzresearch.com/index.php/MZCJ/article/view/297

44. Zeng, R., Li, N., Zhou, X., & Ma, Y. (2021, October). Building a zero-trust security protection system in the environment of the power Internet of Things. In 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT) (pp. 557-560). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9725015

45. Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. Energy Reports, 8, 1309-1320.

https://www.sciencedirect.com/science/article/pii/S2352484721014190

46. Ni, L., Cui, H., Wang, M., Zhi, D., Han, K., & Kou, W. (2022, February). Construction of data center security system based on micro isolation under zero trust architecture. In 2022 2nd Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS) (pp. 113-116). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9820976

47. Russo, S. Industrial Demilitarized Zone and Zero Trust cybersecurity models for Industrial Control Systems.

    https://amslaurea.unibo.it/id/eprint/26737/

48. Colombo, P., Ferrari, E., & Tümer, E. D. (2021, December). Access Control Enforcement in IoT: state of the art and open challenges in the Zero Trust era. In 2021 third ieee international conference on trust, privacy and security in intelligent systems and applications (tps-isa) (pp. 159-166). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9750238

49. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Federated Learning in Zero Trust Security: Decentralized AI for Real-Time Threat Detection and Policy Enforcement.

50. Abbas, N., & Anis, M. (2022). The Future of Cybersecurity: Leveraging AI for Threat Prediction and Zero Trust Defense.

    https://www.researchgate.net/profile/Mirza-Anis/publication/388243361_The_Future_of_Cybersecurity_Leveraging_AI_for_Threat_Prediction_and_Zero_Trust_Defense/links/6790a0c798c4e967fa756a45/The-Future-of-Cybersecurity-Leveraging-AI-for-Threat-Prediction-and-Zero-Trust-Defense.pdf

51. Liu, Z., Li, X., & Mu, D. (2022). Data- Driven Zero Trust Key Algorithm. Wireless Communications and Mobile Computing, 2022(1), 8659428.

    https://onlinelibrary.wiley.com/doi/full/10.1155/2022/8659428

52. Yiliyaer, S., & Kim, Y. (2022, January). Secure access service edge: A zero trust based framework for accessing data securely. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0586-0591). IEEE.

    https://ieeexplore.ieee.org/abstract/document/9720872

53. Kak, S. (2022). Zero Trust Evolution & Transforming Enterprise Security (Doctoral dissertation, California State University San Marcos).

    https://scholarworks.calstate.edu/downloads/7s75dj998

54. Shrivastwa, R. R., Bouakka, Z., Perianin, T., Dislaire, F., Gaudron, T., Souissi, Y., ... & Guilley, S. (2022, October). An embedded AI-based smart intrusion detection system for edge-to-cloud systems. In International Conference on Cryptography, Codes and Cyber Security (pp. 20-39). Cham: Springer Nature Switzerland.

    https://link.springer.com/chapter/10.1007/978-3-031-23201-5_2

55. Dataset Link. https://www.kaggle.com/datasets/veronica4/hornet-40