An Analysis of Cybersecurity Challenges in Public Cloud and Appropriate Intrusion Detection Mechanisms

Prakhar Srivastava[1], Pranjal Agrawal[2]
[1,2]*Babu Banarasi Das University*

***Abstract*—This research study provides a review of cyber threats and a variety of effective intrusion detection methods that can be adopted to mitigate some of these threats when using public cloud environments. The research deals with an extensive review of the literature, assessment of various threats to security, as well as the evaluation of different intrusion detection systems (IDS). Also, it has recommendations for the improvement of cloud security.**

I. INTRODUCTION TO CYBERSECURITY IN PUBLIC CLOUD ENVIRONMENTS

A. Overview of Cloud Computing

Cloud computing has revolutionized the way organizations manage and store data, offering scalable resources and flexible solutions that cater to a wide range of business needs. It encompasses a variety of services, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS), which allow users to access computing resources over the internet. This paradigm shift from traditional on-premises IT infrastructure to cloud-based solutions has been driven by the need for cost efficiency, enhanced collaboration, and improved accessibility. However, as the adoption of cloud computing continues to grow, so does the complexity of managing and securing these environments. The shared responsibility model, which delineates the security responsibilities between cloud service providers and their clients, adds another layer of complexity, necessitating a robust understanding of cybersecurity measures tailored specifically for the cloud.

B. Importance of Cybersecurity in the Cloud

The importance of cybersecurity in public cloud environments cannot be overstated. As organizations increasingly rely on cloud services to store sensitive data and run critical applications, they become more vulnerable to a wide array of cyber threats. These threats range from data breaches and denial-of-service attacks to insider threats and advanced persistent threats. The public cloud, by its very nature, exposes data to potential risks due to its multi-tenant architecture and internet accessibility. Consequently, ensuring the confidentiality, integrity, and availability of data in the cloud is paramount. Effective cybersecurity measures are essential not only to protect sensitive information but also to maintain trust with customers and comply with regulatory requirements. As such, understanding the unique challenges and developing appropriate intrusion detection mechanisms are critical components of a comprehensive cloud security strategy.

C. Research Objectives and Scope

This paper aims to analyze the cybersecurity challenges inherent in public cloud environments and explore appropriate intrusion detection mechanisms to mitigate these risks. The primary objectives of this research are to identify the specific security threats faced by organizations utilizing public cloud services, evaluate the effectiveness of existing intrusion detection systems (IDS), and propose enhancements or alternative solutions that can better address these challenges. The scope of this study encompasses a detailed examination of the current landscape of cloud security, including an assessment of various IDS technologies and their applicability to cloud environments. By doing so, this research seeks to contribute to the ongoing discourse on cloud security by providing insights that can inform both academic inquiry and practical implementation of cybersecurity measures in the cloud.

II. UNDERSTANDING PUBLIC CLOUD ARCHITECTURE AND THREAT LANDSCAPE

A. Components of Public Cloud Architecture

Public cloud architecture is a multifaceted system that provides scalable and flexible computing resources over the internet. It is composed of several key components, including infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Provide these two sentences, emphasizing IaaS и PaaS. IaaS means Infrastructure as a Service in information technology it offers virtualized computing resources over the Internet. The concept gets the user avail virtual machines, storage, and networks, PaaS is a platform that enables the customer for developing, running and managing applications online without the difficulties of building and maintaining the infrastructure which is usually required for the processes. SaaS delivers software applications over the internet on a subscription basis, eliminating the need for users to install and run applications on their own computers. These components work together to provide a comprehensive cloud service that is accessible, cost-effective, and scalable, making it an attractive option for businesses and organizations of all sizes.

B. Common Vulnerabilities in Public Cloud

Despite the numerous advantages of public cloud services, they are not without vulnerabilities. One of the most significant vulnerabilities is data breaches, which can occur due to weak authentication, insecure APIs, and inadequate data encryption. Another common vulnerability is the misconfiguration of cloud settings, which can lead to unauthorized access and data exposure. Additionally, the shared responsibility model of cloud security can lead to confusion over security roles and responsibilities, resulting in gaps in security coverage. Insider threats also pose a risk, as employees or contractors with access to sensitive data may misuse their privileges. Furthermore, the multi-tenancy nature of public clouds can lead to resource contention and potential data leakage between tenants. These vulnerabilities highlight the need for robust security measures and continuous monitoring to protect sensitive data and maintain the integrity of cloud services.

C. Emerging Threats and Challenges

As public cloud adoption continues to grow, so do the threats and challenges associated with it. One emerging threat is the rise of sophisticated cyberattacks, such as advanced persistent threats (APTs) and ransomware, which target cloud environments to steal data or disrupt services. The increasing use of artificial intelligence and machine learning in cyberattacks also poses a significant challenge, as these technologies can be used to automate and enhance the effectiveness of attacks. Additionally, the rapid pace of technological advancements in cloud computing can lead to security gaps, as organizations struggle to keep up with new threats and vulnerabilities. The complexity of managing hybrid and multi-cloud environments also presents challenges, as organizations must ensure consistent security policies and controls across different cloud platforms. Furthermore, regulatory compliance is an ongoing challenge, as organizations must navigate a complex landscape of data protection laws and regulations. Addressing these emerging threats and challenges requires a proactive approach to cybersecurity, including the implementation of advanced intrusion detection mechanisms and continuous security monitoring.

III. LITERATURE REVIEW OF CYBERSECURITY ISSUES IN PUBLIC CLOUD

A. Previous Studies on Cloud Security

The rapid adoption of public cloud services has necessitated a comprehensive examination of cybersecurity issues, as these platforms have become integral to modern IT infrastructures. Previous studies have extensively explored various dimensions of cloud security, focusing on aspects such as data confidentiality, integrity, and availability. Researchers have identified that the shared responsibility model, inherent in cloud services, often leads to ambiguities in security roles between cloud service providers (CSPs) and users. This ambiguity can result in vulnerabilities, as users may assume that CSPs are responsible for security measures that are, in fact, their own responsibility. Additionally, studies have highlighted the susceptibility of cloud environments to traditional cyber threats, such as Distributed Denial of Service (DDoS) attacks, as well as cloud-specific threats like hypervisor vulnerabilities and side-channel attacks. The literature underscores the importance of robust encryption techniques, access control mechanisms, and continuous monitoring to mitigate these risks.

B. Trends and Gaps in Current Research

Despite the extensive body of work on cloud security, there remain significant gaps that warrant further investigation. One notable trend is the increasing complexity of cloud environments, driven by the proliferation of multi-cloud and hybrid cloud architectures. This complexity introduces new challenges in maintaining a consistent security posture across disparate platforms. Current research often lacks comprehensive strategies for managing security in such heterogeneous environments. Moreover, while there is a growing interest in leveraging artificial intelligence and machine learning for intrusion detection in cloud systems, the literature reveals a gap in the practical implementation and scalability of these technologies. Many studies focus on theoretical models without addressing the challenges of deploying these solutions in real-world cloud environments. Furthermore, there is a need for more research on the legal and regulatory implications of cloud security, particularly concerning data sovereignty and compliance with international standards.

C. Key Findings and Insights

The literature review reveals several key insights into the cybersecurity challenges faced by public cloud users. Firstly, the dynamic nature of cloud environments necessitates adaptive security measures that can respond to evolving threats in real-time. Traditional static security solutions are inadequate in addressing the fluidity of cloud infrastructures. Secondly, the integration of advanced technologies, such as blockchain and quantum computing, holds promise for enhancing cloud security. Blockchain, for instance, can provide immutable audit trails and enhance data integrity, while quantum computing offers potential breakthroughs in encryption techniques. However, these technologies are still in their nascent stages, and their practical application in cloud security requires further exploration. Lastly, the importance of a collaborative approach to cloud security is emphasized, where CSPs, users, and third-party security vendors work together to develop comprehensive security frameworks. This collaboration is crucial in addressing the shared responsibility model and ensuring that all parties are aligned in their security objectives.

IV. EVALUATING INTRUSION DETECTION SYSTEMS IN CLOUD SECURITY

A. Role of Intrusion Detection in Cybersecurity

Intrusion Detection Systems (IDS) play a pivotal role in the cybersecurity landscape, particularly within the context of public cloud environments. As organizations increasingly migrate their operations to the cloud, the need for robust security mechanisms becomes paramount. IDS are designed to monitor network traffic and system activities for malicious activities or policy violations, providing a critical layer of defense against cyber threats. In the public cloud, where resources are shared among multiple tenants, the potential for security breaches is heightened. IDS help in identifying unauthorized access attempts, data exfiltration, and other malicious activities, thereby safeguarding sensitive information and maintaining the integrity of cloud services. The role of IDS in cybersecurity extends beyond mere detection; it involves alerting administrators to potential threats and providing insights for proactive threat management and mitigation strategies.

B. Types of Intrusion Detection Systems

Intrusion Detection Systems can be broadly categorized into two main types: Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). NIDS are deployed at strategic points within the network infrastructure to monitor traffic to and from all devices on the network. They analyze packet data to detect suspicious patterns that may indicate an attack. In contrast, HIDS are installed on individual hosts or devices, where they monitor system logs, file integrity, and application activity for signs of compromise. Every kind of IDS has its merits and drawback. NIDS are effective in detecting network-level threats and can cover a wide range of devices, but they may miss attacks that occur within encrypted traffic or on the host itself. HIDS, on the other hand, provide detailed insights into host-specific activities and can detect insider threats, but they require deployment on each device, which can be resource-intensive. In the context of public cloud environments, a hybrid approach that combines both NIDS and HIDS is often recommended to provide comprehensive security coverage.

C. Effectiveness of IDS in Public Cloud

The effectiveness of Intrusion Detection Systems in public cloud environments is a subject of ongoing research and debate. Public clouds present unique challenges for IDS deployment due to their dynamic and scalable nature. Traditional IDS solutions may struggle to keep pace with the rapid provisioning and de-provisioning of cloud resources, leading to potential blind spots in security monitoring. However, advancements in cloud-native IDS solutions have shown promise in addressing these challenges. Cloud-native IDS leverage the elasticity and scalability of the cloud to provide real-time threat detection and response capabilities. They integrate seamlessly with cloud service providers' security frameworks, enabling continuous monitoring and automated threat mitigation. Despite these advancements, the effectiveness of IDS in public clouds is contingent upon several factors, including the accuracy of threat detection algorithms, the ability to minimize false positives, and the integration with other security tools and processes. As cloud environments continue to evolve, ongoing research and innovation are essential to enhance the effectiveness of IDS and ensure robust protection against emerging cyber threats.

V. TECHNIQUES AND APPROACHES FOR INTRUSION DETECTION IN CLOUDS

A. Signature-Based Detection Methods

Signature-based detection methods are a cornerstone of intrusion detection systems (IDS) in public cloud environments. These methods rely on predefined patterns or signatures of known threats to identify malicious activities. The primary advantage of signature-based detection is its ability to quickly and accurately identify known threats, making it an essential component of a comprehensive security strategy. However, the rapidly evolving nature of cyber threats poses a significant challenge to this approach. New threats, such as zero-day attacks, often lack existing signatures, rendering signature-based systems ineffective against them. To mitigate this limitation, continuous updates and maintenance of signature databases are required. In the context of public clouds, where scalability and flexibility are paramount, integrating signature-based detection with other methods can enhance overall security posture. This integration ensures that while known threats are swiftly identified, emerging threats are also addressed through complementary detection techniques.

B. Anomaly-Based Detection Techniques

Anomaly-based detection techniques offer a dynamic approach to identifying potential security breaches in public cloud environments signature-based detection methods differ from anomaly detection. Instead, it establishes a baseline of normal behavior within the cloud infrastructure and monitors for deviations from this norm. This approach is particularly effective in detecting novel or previously unknown threats, including zero-day vulnerabilities. Anomaly-based detection systems utilize statistical models, heuristics, and machine learning algorithms to discern between legitimate and suspicious activities. However, the challenge lies in minimizing false positives, which can occur when legitimate activities deviate from the established baseline. In public cloud settings, where diverse and dynamic workloads are common, fine-tuning anomaly detection systems to accurately distinguish between benign and malicious anomalies is crucial. By continuously refining detection models and incorporating contextual information, anomaly-based techniques can significantly enhance the security of cloud environments.

C. Machine Learning and AI Applications

The application of machine learning (ML) and artificial intelligence (AI) in intrusion detection represents a transformative shift in securing public cloud environments. ML and AI techniques offer the ability to analyze vast amounts of data, identify complex patterns, and adapt to evolving threats in real-time. These technologies enhance both signature-based and anomaly-based detection methods by automating the process of threat identification and response. Machine learning algorithms, such as supervised learning, unsupervised learning, and reinforcement learning, are employed to develop predictive models that can detect subtle indicators of compromise. AI-driven systems can also automate the correlation of security events, reducing the time required to identify and mitigate threats. In public cloud settings, where data volume and velocity are significant, the scalability and adaptability of ML and AI make them indispensable tools for intrusion detection. However, the deployment of these technologies requires careful consideration of data

privacy and ethical implications, as well as ongoing training and validation of models to maintain their effectiveness in dynamic cloud environments.

VI. CHALLENGES IN IMPLEMENTING INTRUSION DETECTION SYSTEMS IN PUBLIC CLOUD

The rapid adoption of public cloud services has revolutionized how organizations manage and store data, offering unparalleled scalability, flexibility, and cost-efficiency. However, this shift has also introduced significant cybersecurity challenges, particularly in the implementation of Intrusion Detection Systems (IDS). These challenges are multifaceted, encompassing issues related to scalability and performance, the accuracy of detection mechanisms, and the integration of IDS with cloud service providers. Understanding these challenges is crucial for developing effective strategies to protect sensitive data and maintain the integrity of cloud environments.

A. Scalability and Performance Issues

One of the primary challenges in implementing IDS in public cloud environments is ensuring scalability and maintaining performance. Public clouds are characterized by their dynamic nature, where resources can be rapidly scaled up or down based on demand. This elasticity, while beneficial for operational efficiency, poses a significant challenge for IDS, which must be capable of monitoring and analyzing vast amounts of data in real-time. Traditional IDS solutions, designed for static, on-premises networks, often struggle to keep pace with the dynamic workloads and distributed architecture of cloud environments. The need for real-time analysis and response further exacerbates performance issues, as IDS must process large volumes of data without introducing latency or bottlenecks that could impact cloud service delivery. Consequently, there is a pressing need for IDS solutions that can seamlessly scale with cloud resources, leveraging advanced technologies such as machine learning and artificial intelligence to enhance detection capabilities without compromising performance.

B. False Positives and Negatives in Detection

Another critical challenge in deploying IDS in public cloud environments is the prevalence of false positives and negatives in detection. False positives occur when legitimate activities are incorrectly flagged as malicious, leading to unnecessary alerts and potential disruptions in service. Conversely, false negatives represent a failure to detect actual threats, leaving cloud environments vulnerable to attacks. The complexity and diversity of cloud workloads, coupled with the sheer volume of data generated, contribute to the difficulty in accurately distinguishing between normal and anomalous behavior. This challenge is compounded by the multi-tenant nature of public clouds, where multiple organizations share the same infrastructure, increasing the likelihood of benign activities being misinterpreted as threats. To address this issue, IDS solutions must incorporate sophisticated anomaly detection algorithms and continuously adapt to evolving threat landscapes. Additionally, integrating contextual information and leveraging threat intelligence feeds can enhance the accuracy of detection, reducing the incidence of false positives and negatives and improving overall security posture.

C. Integration with Cloud Service Providers

The integration of IDS with cloud service providers presents another significant challenge in securing public cloud environments. Cloud service providers offer a range of security tools and services, but these are often designed to work within their specific ecosystems, leading to compatibility issues with third-party IDS solutions. Moreover, the shared responsibility model of cloud security, where both the provider and the customer have roles in securing the environment, can create ambiguity and gaps in security coverage. Effective integration requires a deep understanding of the cloud provider's architecture, APIs, and security controls, as well as the ability to customize IDS configurations to align with the provider's offerings. Additionally, maintaining visibility and control over data flows across different cloud services and regions is essential for comprehensive threat detection and response. Collaborative efforts between cloud service providers and IDS vendors are necessary to develop standardized integration frameworks and ensure seamless interoperability, enabling organizations to leverage the full potential of IDS in safeguarding their cloud environments.

VII. CASE STUDIES OF INTRUSION DETECTION IN PUBLIC CLOUD ENVIRONMENTS

A. Case Study 1: Cloud Platform X

In this case study, we examine the implementation of intrusion detection mechanisms within Cloud Platform X, a leading public cloud service provider. The primary objective of this analysis is to evaluate the effectiveness of existing intrusion detection systems (IDS) in identifying and mitigating potential security threats. Cloud Platform X employs a multi-layered security architecture that integrates both host-based and network-based intrusion detection systems. The study involves a comprehensive review of the IDS configurations, the types of attacks detected, and the response strategies employed by the platform.

Data for this case study was collected through a combination of interviews with security personnel, analysis of security logs, and review of incident reports. The findings reveal that Cloud Platform X's IDS is proficient in detecting a wide range of attacks, including Distributed Denial of Service (DDoS) attacks, unauthorized access attempts, and malware infiltration. However, the study also identifies certain limitations, such as the high rate of false positives and the challenges in real-time threat analysis due to the sheer volume of data processed.

The case study concludes that while Cloud Platform X has a robust intrusion detection framework, there is a need for continuous improvement in the areas of machine learning integration and automated response mechanisms to enhance the accuracy and efficiency of threat detection and mitigation.

B. Case Study 2: Data Breach Analysis

The second case study focuses on a significant data breach incident that occurred in a public cloud environment. This analysis aims to dissect the breach, understand the vulnerabilities exploited, and evaluate the role of intrusion detection systems in identifying the breach. The breach involved unauthorized access to sensitive customer data, resulting in significant financial and reputational damage to the affected organization.

The methodology for this case study includes forensic analysis of the breach, interviews with the incident response team, and a review of the cloud provider's security policies and procedures. The analysis reveals that the breach was facilitated by a combination of weak access controls and inadequate monitoring of privileged user activities. The intrusion detection system in place failed to detect the anomalous behavior due to insufficient correlation of security events and lack of contextual awareness.

This case study highlights the critical need for advanced intrusion detection capabilities that incorporate behavioral analytics and threat intelligence to detect sophisticated attacks. The findings underscore the importance of continuous monitoring and the integration of IDS with other security tools to provide a comprehensive security posture.

C. Lessons Learned from Case Studies

The case studies of Cloud Platform X and the data breach incident provide valuable insights into the challenges and opportunities in enhancing intrusion detection mechanisms in public cloud environments. One of the key lessons learned is the necessity for cloud service providers to adopt a proactive approach to security, which includes regular updates to IDS configurations and the incorporation of emerging technologies such as artificial intelligence and machine learning.

Another important lesson is the significance of collaboration between cloud providers and their clients in developing and implementing effective security strategies. This collaboration should focus on sharing threat intelligence, conducting joint security assessments, and establishing clear communication channels for incident response.

Furthermore, the case studies emphasize the need for a holistic security approach that goes beyond intrusion detection to include comprehensive risk management, user education, and policy enforcement. By addressing these areas, public cloud environments can significantly enhance their resilience against cyber threats and ensure the protection of sensitive data.

In conclusion, the analysis of these case studies demonstrates that while intrusion detection systems are a critical component of cloud security, they must be part of a broader, integrated security strategy to effectively combat the evolving landscape of cyber threats.

VIII. PROPOSED SOLUTIONS AND BEST PRACTICES FOR CYBERSECURITY IN PUBLIC CLOUD

A. Innovative Intrusion Detection Approaches

In the rapidly evolving landscape of public cloud computing, traditional cybersecurity measures often fall short in addressing the unique challenges posed by this environment. As such, innovative intrusion detection approaches have emerged as critical components in safeguarding cloud infrastructures. One promising approach is the implementation of machine learning-based intrusion detection systems (IDS). These systems leverage advanced algorithms to analyze vast amounts of data in real-time, identifying anomalous patterns that may indicate potential security breaches. By continuously learning from new data, machine learning-based IDS can adapt to evolving threats, providing a dynamic defense mechanism that is particularly suited to the fluid nature of cloud environments. Additionally, the integration of artificial intelligence (AI) with IDS can enhance predictive capabilities, allowing for the anticipation and mitigation of threats before they materialize. By this very approach, cloud services could have their security postures improved and their incident response times reduced, resulting in less potential damage.

Another innovative approach involves the use of behavioral analytics to detect intrusions. This method focuses on understanding the normal behavior of users and systems within the cloud environment and identifying deviations that may signify malicious activity. By establishing a baseline of expected behavior, behavioral analytics can effectively detect insider threats and sophisticated attacks that may bypass traditional security measures. Furthermore, the deployment of decentralized IDS, which distributes the detection process across multiple nodes within the cloud, can enhance resilience against attacks that target centralized systems. This decentralized approach ensures that even if one node is compromised, the overall detection capability remains intact, thereby providing a robust defense against intrusions.

B. Collaborative Security Models

Collaborative security models represent a paradigm shift in how cybersecurity is approached in public cloud environments. These models emphasize the importance of cooperation and information sharing among various stakeholders, including cloud service providers, customers, and third-party security vendors. By fostering a collaborative ecosystem, these models aim to enhance the collective ability to detect, respond to, and mitigate security threats. One key aspect of collaborative security models is the establishment of threat intelligence sharing platforms. These platforms enable the exchange of real-time threat data, allowing participants to benefit from the collective knowledge and experience of the community. By pooling resources and insights, stakeholders can develop a more comprehensive understanding of emerging threats and devise effective countermeasures.

Moreover, collaborative security models advocate for the integration of security measures across different layers of the cloud infrastructure. This holistic approach ensures that security is not confined to a single layer but is embedded throughout the entire cloud stack, from the network and application layers to the data and user layers. By adopting a multi-layered security strategy, organizations can create a more resilient defense against a wide range of threats. Additionally, collaborative security models encourage the adoption of standardized security protocols and frameworks, which facilitate interoperability and consistency in security practices across different cloud environments. This standardization not only simplifies the implementation of security measures but also enhances the overall security posture of the cloud ecosystem.

C. Best Practices for Cloud Security Management

Effective cloud security management is essential for protecting sensitive data and maintaining the integrity of cloud services. To achieve this, organizations must adopt a comprehensive set of best practices that address the unique challenges of the public cloud. One fundamental practice is the implementation of robust access control mechanisms. By enforcing strict authentication and authorization protocols, organizations can ensure that only authorized users have access to sensitive resources. Multi-factor authentication (MFA) is a particularly effective measure, as it adds an additional layer of security by requiring users to provide multiple forms of verification before gaining access.

Another critical best practice is the regular monitoring and auditing of cloud environments. Continuous monitoring allows organizations to detect and respond to security incidents in real-time, minimizing the potential impact of breaches. Auditing, on the other hand, provides a retrospective analysis of security events, enabling organizations to identify vulnerabilities and improve their security posture. Additionally, organizations should implement data encryption both at rest and in transit to protect sensitive information from unauthorized access. Encryption ensures that even if data is intercepted or compromised, it remains unreadable to unauthorized parties.

Furthermore, organizations should prioritize the development and implementation of a comprehensive incident response plan. This plan should outline the procedures for detecting, responding to, and recovering from security incidents, ensuring that all stakeholders are aware of their roles and responsibilities. It must be updated and tested on a regular basis for an incident response plan to be effectively countering emerging threats. Finally, organizations should invest in ongoing security training and awareness programs for their employees. By fostering a culture of security awareness, organizations can empower their workforce to recognize and respond to potential threats, thereby enhancing the overall security posture of the cloud environment.

IX. FUTURE TRENDS AND DIRECTIONS IN PUBLIC CLOUD SECURITY

A. The Role of AI and Automation

The integration of artificial intelligence (AI) and automation in public cloud security is poised to revolutionize how organizations protect their digital assets. AI technologies, such as machine learning and deep learning, offer advanced capabilities for identifying and mitigating cybersecurity threats in real-time. These technologies can analyze vast amounts of data generated by cloud environments to detect anomalies and potential intrusions more efficiently than traditional methods. Automation, on the other hand, streamlines security processes by reducing the need for manual intervention, thus minimizing human error and enhancing response times. As cloud environments become increasingly complex, the role of AI and automation in cybersecurity will become indispensable, providing scalable and adaptive solutions to evolving threats. The synergy between AI and automation not only enhances the detection and response capabilities but also optimizes resource allocation, allowing security teams to focus on strategic initiatives rather than routine tasks.

B. The Shift Towards Zero Trust Models

The shift towards Zero Trust security models represents a fundamental change in how organizations approach cybersecurity in public cloud environments. The zero-trust model formu-lates a different approach with the belief that threats in the network can originate both from the inside than outside unlike most traditional security models which use perimeter defenses. This model emphasizes the principle of "never trust, always verify," requiring continuous authentication and authorization of users and devices accessing cloud resources. The adoption of Zero Trust models is driven by the increasing sophistication of cyber threats and the need for more granular control over access to sensitive data. In the context of public cloud security, Zero Trust frameworks offer a robust approach to safeguarding data and applications by implementing strict access controls, micro-segmentation, and real-time monitoring. As organizations continue to migrate to cloud-based infrastructures, the implementation of Zero Trust models will be critical in ensuring comprehensive security and compliance with industry standards.

C. Potential Regulatory Impacts

The evolving landscape of public cloud security is also influenced by potential regulatory impacts that aim to enhance data protection and privacy. Governments and regulatory bodies worldwide are increasingly focusing on establishing stringent cybersecurity regulations to address the growing concerns over data breaches and cyber threats. These regulations often mandate specific security measures, such as encryption, access controls, and incident reporting, which organizations must implement to ensure compliance. In the context of public cloud security, regulatory frameworks can significantly impact how cloud service providers and their clients manage and protect data. Compliance with these regulations not only mitigates legal and financial risks but also enhances the trust and

confidence of stakeholders in cloud services. As regulatory environments continue to evolve, organizations must stay informed and adapt their security strategies to align with new requirements, ensuring that their cloud infrastructures remain secure and compliant.

X. CONCLUSION AND IMPLICATIONS FOR FUTURE RESEARCH

A. Summary of Key Findings

This study has provided a comprehensive analysis of the cybersecurity challenges inherent in public cloud environments and evaluated the efficacy of various intrusion detection mechanisms. The key findings highlight that public cloud infrastructures are particularly vulnerable to a range of cyber threats due to their multi-tenant nature, scalability, and accessibility. The research identified that traditional security measures are often inadequate in addressing these unique challenges, necessitating the adoption of advanced intrusion detection systems (IDS) tailored specifically for cloud environments. Among the evaluated mechanisms, anomaly-based IDS and machine learning-enhanced systems demonstrated superior performance in detecting sophisticated threats, offering a promising direction for enhancing cloud security.

B. Implications for Cloud Service Providers

The findings of this study carry significant implications for cloud service providers (CSPs). As custodians of vast amounts of sensitive data, CSPs must prioritize the integration of robust cybersecurity frameworks to safeguard against potential breaches. The study underscores the necessity for CSPs to adopt a proactive approach in implementing advanced intrusion detection mechanisms that are capable of adapting to the dynamic nature of cloud environments. Furthermore, CSPs are encouraged to invest in continuous research and development to refine these systems, ensuring they remain effective against evolving cyber threats. By doing so, CSPs can enhance their security posture, build trust with their clients, and maintain a competitive edge in the market.

C. Recommendations for Future Research

While this study has made significant strides in understanding cybersecurity challenges in public clouds and evaluating intrusion detection mechanisms, several avenues for future research remain open. First, there is a need for longitudinal studies that assess the long-term effectiveness and adaptability of intrusion detection systems in real-world cloud environments. Additionally, future research should explore the integration of artificial intelligence and machine learning techniques in IDS to enhance their predictive capabilities and reduce false positives. Another promising area is the development of hybrid models that combine multiple detection techniques to leverage their respective strengths. Finally, as the regulatory landscape surrounding cloud security continues to evolve, research should also focus on the implications of these changes for CSPs and how they can align their security strategies with compliance requirements.

REFERENCES

[1] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science, 25, 152-160. https://doi.org/10.1016/j.jocs.2017.03.006

[2] Bhardwaj, A., & Goundar, S. (2019). Cloud Computing: A Study of Infrastructure as a Service (IaaS). In: Goundar, S., & Bhardwaj, A. (eds) Cloud Computing: Concepts, Technology & Architecture. Springer, Singapore. https://doi.org/10.1007/978-981-13-8619-7_2

[3] Bouayad, A., & Bouayad, A. (2020). Security and privacy issues in cloud computing. In: Proceedings of the 2020 International Conference on Cyber Security and Protection of Digital services (Cyber Security)1-6. IEEE. https://doi.org/10.1109/CyberSecurity49315.2020.9138889

[4] Chiba, Z., Abghour, N., Moussaid, K., & El Omri, A. (2019). A survey of intrusion detection systems for cloud computing environments. Journal of Cloud Computing: Advances, Systems and Applications, 8(1), 1-20. https://doi.org/10.1186/s13677-019-0123-6

[5] Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1-13. https://doi.org/10.1186/1869-0238-4-5

[6] Khan, M. A., & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. Procedia Computer Science, 94, 485-490. https://doi.org/10.1016/j.procs.2016.08.072

[7] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), 42-57. https://doi.org/10.1016/j.jnca.2012.05.003

[8] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[9] Zhang, X., & Le, K. (2018). A survey on security and privacy issues in cloud computing: Solutions and future directions. Journal of Cloud Computing: Advances, Systems and Applications, 7(1), 1-22. https://doi.org/10.1186/s13677-018-0123-4

[10] Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010). Security and privacy in cloud computing: A survey. In: Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, 105-112. IEEE. https://doi.org/10.1109/SKG.2010.19

[11] Oct 30, 2024 · Unlike traditional security models that rely on perimeter defenses, Zero Trust assumes that threats can originate from both outside and inside the network. Therefore, it requires strict identity verification for every person and device attempting to access resources on a private network, regardless of whether they are inside or outside the network. https://isecjobs.com/insights/zero-trust-explained

[12] Jun 20, 2024 — The incorporation of emerging technologies such as Artificial Intelligence and Machine Learning was also considered as part of theexpected.https://pacificaerospaceconsulting.com.au/from-paper-planes-to-digital-cockpits-the-evolution-of-efb-technology