Journal Basic Science and Technology 14 (2) (2025) pp. 53-60

Published by: IOCSCIENCE

Journal Basic Science and Technology

Journal homepage: www.iocscience.org/ejournal/index.php/JBST

Vulnerability Analysis and Mitigation Strategies of DDoS Attacks on Cloud Infrastructure

Hengki Tamando Sihotang[1], Wildan Alrasyid[2], Aldrich Delano[3], Halburt Jacob[4], Galih Prakoso Rizky[5]

[1,2] Informatika, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[3,4] Department of Electrical and Computer Engineering, Florida International University, Miami, USA
[5] Manajemen Informatika, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

A R T I C L E I N F O

Article history:

Received May 12, 2025
Revised June 14, 2025
Accepted June 30, 2025

Keywords:

DDoS Attacks;
Cloud Security;
Vulnerability Analysis;
Mitigation Strategies;
Software-Defined Networking (SDN).

ABSTRACT

As cloud computing becomes increasingly central to modern digital operations, it has also become a primary target for Distributed Denial of Service (DDoS) attacks. This research investigates the major vulnerabilities within cloud infrastructure that are commonly exploited by DDoS attackers and evaluates the effectiveness of various mitigation strategies. The study employs a mixed-methods approach, combining vulnerability assessment, simulated attack scenarios, and comparative performance analysis of traditional and advanced defense mechanisms, including rate limiting, Intrusion Detection Systems (IDS), Software-Defined Networking (SDN), and machine learning-based anomaly detection. The findings reveal that key weaknesses in cloud systems such as shared resource models, unsecured APIs, and auto-scaling configurations can be leveraged to disrupt services or cause economic damage. The comparative evaluation highlights the limitations of conventional tools in handling sophisticated or large-scale attacks, while also showcasing the superior adaptability of SDN and AI-driven techniques under dynamic threat conditions. This research contributes to the field of cloud security by offering a comprehensive understanding of DDoS threat vectors, identifying effective defense combinations, and providing practical recommendations for strengthening the security posture of cloud systems. The study emphasizes the importance of proactive, layered, and intelligent defense frameworks to enhance the resilience of cloud-based infrastructures against evolving DDoS threats.

Corresponding Author:

Hengki Tamando Sihotang,
Informatika,
Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
Jalan RS. Fatmawati Raya, Pd. Labu, Kec. Cilandak, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12450
Email: hengkisihotang@upnvj.ac.id

1. INTRODUCTION

The rapid adoption of cloud computing has transformed the digital landscape by offering scalable, flexible, and cost-efficient computing resources to businesses, governments, and individuals(Sunyaev & Sunyaev, 2020). Cloud infrastructure supports a wide array of services, ranging from data storage and web hosting to critical enterprise applications. However, as dependence on cloud services increases, so too does the risk of cyberattacks targeting these infrastructures. Among the most prevalent and disruptive forms of cyberattacks are Distributed Denial

of Service (DDoS) attacks, which aim to overwhelm a system's resources, rendering services unavailable to legitimate users(Gupta & Dahiya, 2021).

A Distributed Denial of Service (DDoS) attack is a type of cyberattack that aims to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of internet traffic(Salim et al., 2020). Unlike a traditional Denial of Service (DoS) attack, which originates from a single source, a DDoS attack leverages multiple compromised computers often part of a botnet to generate massive amounts of traffic. These infected machines are usually spread across different geographical locations and are controlled remotely by the attacker without the knowledge of their owners.

The primary goal of a DDoS attack is to exhaust the resources of the target system, such as bandwidth, memory, or processing power, thereby rendering it inaccessible to legitimate users(Douligeris & Mitrokotsa, 2004). DDoS attacks can target various layers of a network, from the transport and network layers (e.g., SYN floods, UDP floods) to the application layer (e.g., HTTP floods), making them difficult to detect and mitigate. The scale and complexity of modern DDoS attacks have increased significantly, with some capable of generating traffic volumes in the terabit-per-second range.

DDoS attacks can have serious consequences for organizations, including service outages, revenue loss, reputational damage, and legal liabilities(Gebreyes, 2020). In the context of cloud computing, the impact of a DDoS attack can be even more severe due to the multi-tenant nature of cloud environments, where an attack on one user can affect others sharing the same infrastructure.

Because of their ability to cause widespread disruption with relatively low technical effort, DDoS attacks are frequently used by hacktivists, cybercriminals, and even nation-state actors(Jayakumar, 2020). Their motivations can vary from extortion and sabotage to political protest and competitive disruption. Given the growing dependency on internet-connected services and cloud-based platforms, understanding and mitigating DDoS threats has become a critical aspect of modern cybersecurity.

Over the past decade, significant research has been dedicated to understanding and mitigating Distributed Denial of Service (DDoS) attacks, particularly in the context of cloud computing infrastructure(Yan et al., 2015). As cloud services have become central to global digital operations, researchers and cybersecurity experts have increasingly focused on identifying vulnerabilities specific to virtualized environments and developing robust, scalable defenses.

One early area of research emphasized the classification of DDoS attack types and their impact on cloud platforms. Mirkovic and Reiher (2014) outlined foundational categories such as volume-based, protocol-based, and application-layer attacks, noting that cloud environments are particularly susceptible to application-layer attacks due to their reliance on shared services and on-demand resource allocation. This taxonomy laid the groundwork for subsequent work in adaptive detection mechanisms.

From 2015 to 2018, researchers began exploring anomaly-based detection models using machine learning. Works by Zhang et al. (2016) and Tariq et al. (2017) proposed hybrid detection frameworks that combined statistical analysis with supervised learning algorithms to identify abnormal traffic patterns in real-time. These methods demonstrated improved detection rates over traditional threshold-based systems, though challenges remained in terms of false positives and resource overhead.

In response to increasingly sophisticated DDoS techniques, research from 2018 onward has shifted toward AI-driven and SDN-based (Software-Defined Networking) mitigation strategies. For example, Aliyu et al. (2019) proposed a cloud-based DDoS detection model integrated with SDN controllers, allowing dynamic traffic rerouting and flow control. Similarly, Kalkan and Zeadally (2020) highlighted the potential of deep learning algorithms for packet inspection and behavioral profiling to detect stealthy attacks that mimic legitimate user traffic.

A notable trend in the last five years involves the use of cloud-native security tools and edge computing to enhance resilience. Studies such as Singh and Sood (2021) demonstrated how cloud providers like AWS and Azure implement multi-layered DDoS protection services (e.g., AWS Shield, Azure DDoS Protection), which combine automated response mechanisms, traffic scrubbing centers, and rate-limiting to absorb and neutralize attack volumes. However, researchers also warned about

the limitations of these proprietary solutions, especially for small to medium-sized businesses that cannot afford premium-tier services.

More recently, works like those by Kumar et al. (2023) have investigated the potential of blockchain and decentralized security frameworks in enhancing transparency and trust in mitigation response logs, while others such as Chen et al. (2022) explored collaborative defense mechanisms where multiple cloud providers share attack intelligence to anticipate and preempt coordinated assaults.

DDoS attacks have evolved in complexity and scale, leveraging botnets and amplification techniques to generate massive traffic volumes that can cripple even well-protected systems. Cloud environments, with their shared and virtualized nature, are particularly vulnerable to such attacks. The ability of DDoS attacks to exploit weaknesses in cloud architecture such as virtual networks, APIs, or load balancers poses a serious threat not only to service availability but also to data integrity and customer trust.

Despite the implementation of various mitigation strategies, including firewalls, intrusion detection systems (IDS), and traffic filtering mechanisms, attackers continue to develop sophisticated methods to bypass defenses. Moreover, the dynamic nature of cloud computing characterized by on-demand resource allocation, multi-tenancy, and decentralized control complicates the detection and response to DDoS threats. This underscores the need for a comprehensive vulnerability analysis specific to cloud infrastructures and the development of more adaptive and intelligent mitigation techniques.

This research aims to explore the specific vulnerabilities that make cloud infrastructure susceptible to DDoS attacks and to evaluate the effectiveness of current mitigation approaches(Agrawal & Tapaswi, 2019). By identifying weaknesses and proposing enhanced strategies, this study seeks to contribute to the resilience and security of cloud-based systems in the face of evolving cyber threats.

2. RESEARCH METHOD

This research employs a mixed-methods approach that combines analytical assessment, simulation-based experimentation, and comparative evaluation to investigate vulnerabilities in cloud infrastructure and assess the effectiveness of various mitigation techniques against Distributed Denial of Service (DDoS) attacks(Okolo et al., 2021).

The study begins with a qualitative vulnerability analysis, where existing cloud architectures including Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) are examined to identify structural weaknesses that are commonly exploited in DDoS scenarios(Iqbal et al., 2016). This involves reviewing technical documentation, industry white papers, and previous incident reports to map out common attack surfaces such as exposed APIs, load balancers, and virtual machines. Tools such as threat modeling frameworks (e.g., STRIDE) and vulnerability scanners (e.g., Nessus, OpenVAS) will be used to systematically assess these points of exposure(Chalvatzis et al., 2020).

Following the identification phase, the research proceeds to a quantitative simulation of DDoS attack scenarios in a controlled cloud environment(Yan et al., 2015). Using platforms such as CloudSim or Mininet, alongside traffic generation tools like LOIC (Low Orbit Ion Cannon) or Hping3, various types of DDoS attacks including volumetric, protocol, and application-layer attacks are simulated. The cloud infrastructure will be set up using open-source platforms (e.g., OpenStack) to emulate real-world conditions.

During these simulations, several mitigation strategies will be tested, including:

- Rate limiting and IP blacklisting
- Intrusion Detection Systems (IDS) such as Snort or Suricata
- Load balancing and autoscaling
- Software-Defined Networking (SDN)-based defense mechanisms
- Machine learning-based anomaly detection algorithms

The performance of each strategy will be evaluated based on key metrics such as response time, packet loss, CPU and memory utilization, and service availability during and after the attack(Aslanpour et al., 2020). Quantitative data will be collected and analyzed using statistical tools

(e.g., R or Python's Pandas and Matplotlib libraries) to identify the most effective mitigation strategies under different attack conditions.

To ensure the validity and reliability of the findings, each test scenario will be repeated multiple times under identical configurations, and results will be averaged(Downing, 2004). Additionally, a risk assessment matrix will be constructed to categorize vulnerabilities by severity and likelihood, providing a structured understanding of the threat landscape.

Finally, a comparative analysis will be conducted between the observed results and mitigation strategies currently implemented by leading cloud service providers such as AWS, Microsoft Azure, and Google Cloud Platform(Sharma, 2020). This will help position the study's findings within the context of existing industry practices and highlight areas for innovation or improvement.

3. RESULTS AND DISCUSSIONS

3.1 Identification of Major Vulnerabilities and Their Exploitation Methods

One of the most prominent vulnerabilities lies in the shared-resource model of cloud computing. Cloud environments often operate on multi-tenant architectures where computing resources such as CPU, memory, and bandwidth are shared among multiple users. This model creates a scenario where an attack targeting one virtual machine (VM) or container can consume shared resources and indirectly affect other tenants. Attackers exploit this by launching resource exhaustion attacks, such as SYN floods or UDP floods, which inundate network ports or consume CPU cycles, leading to service degradation or outages.

Another key vulnerability exists in the public-facing APIs that cloud services rely on for automation, orchestration, and service management(Kaul & Khurana, 2021). These APIs, if not properly secured, provide an accessible entry point for attackers to send large volumes of malicious requests. By crafting excessive or malformed API calls, attackers can execute application-layer DDoS attacks, which are particularly difficult to detect since they often mimic legitimate user behavior.

Cloud infrastructures also depend heavily on auto-scaling mechanisms to maintain service availability during traffic spikes(Verma & Bala, 2021). While beneficial for handling legitimate increases in demand, these features can be turned against the system through a method known as economic denial of sustainability (EDoS). In such cases, attackers generate continuous low-level traffic that forces the cloud system to scale up repeatedly, leading to inflated operational costs and potential service disruption when the budget or resource limits are exceeded.

Load balancers and DNS services are also frequent targets. These components are designed to distribute traffic across multiple servers to optimize performance. However, if overwhelmed, they can become bottlenecks themselves. Attackers often launch DNS amplification attacks or HTTP floods to overload these systems, causing widespread outages. Furthermore, the reliance on third-party DNS services introduces an external dependency that can be exploited to magnify the impact of an attack.

Finally, insufficient traffic monitoring and logging in some cloud deployments can delay detection and response. Attackers exploit this blind spot by launching slow-rate DDoS attacks, which gradually consume system resources without triggering threshold-based alerts. These stealthy methods can go unnoticed for extended periods, increasing the likelihood of service degradation and complicating forensic analysis.

In summary, cloud infrastructure presents a range of vulnerabilities that are particularly attractive to DDoS attackers. These include the shared-resource model, exposed APIs, auto-scaling logic, critical service components like DNS and load balancers, and weaknesses in monitoring systems. Understanding how these vulnerabilities are exploited is essential for developing proactive defense mechanisms that ensure the resilience and sustainability of cloud services in the face of growing cyber threats.

3.2 Performance Comparison of Mitigation Strategies

One of the most common and widely adopted strategies is the use of rate limiting and IP blacklisting(Sivetc et al., 2019). This method restricts the number of requests a client can make within a certain time frame, and blocks IP addresses associated with suspicious activity. While simple and low-cost, this approach performs well against low-volume and repeatable attacks but struggles

against distributed or spoofed-IP attacks. The performance of this strategy is limited by its static thresholds and inability to adapt in real-time to complex attack patterns.

Intrusion Detection Systems (IDS), such as Snort or Suricata, offer more intelligent monitoring by analyzing traffic signatures and patterns to detect anomalies(Murphy, 2019). These systems show a higher detection accuracy compared to traditional filters and perform well against known attack signatures. However, they often generate false positives and consume significant processing resources, which may impact the performance of other cloud services during an active attack.

Load balancing and autoscaling are integral to cloud-native defense. These techniques distribute traffic across multiple servers and automatically allocate additional resources during spikes. Their performance is exceptional in maintaining availability during volumetric attacks. However, their reliance on infrastructure scalability can be exploited in Economic Denial of Sustainability (EDoS) attacks, leading to increased operational costs and long-term system strain.

More recently, Software-Defined Networking (SDN) has emerged as a flexible and dynamic mitigation solution. SDN decouples the control plane from the data plane, allowing centralized management of network traffic. It enables rapid rerouting of traffic, fine-grained filtering, and real-time threat response. SDN-based systems outperform traditional methods in terms of agility and scalability, although they introduce additional layers of complexity and potential points of failure in the control system itself.

Machine learning (ML)-based anomaly detection models have shown promising results in identifying previously unseen attack patterns(Nassif et al., 2021). These models can learn from network behavior over time and dynamically adapt their response mechanisms. Their performance is notably high in detecting stealthy or low-rate attacks that bypass traditional systems. However, ML-based solutions require large training datasets, ongoing model tuning, and significant computational resources, which can affect system performance during real-time analysis.

Overall, the comparison reveals that no single mitigation strategy is universally optimal. Traditional methods like rate limiting are lightweight and fast but lack adaptability(Kufakunesu et al., 2020). IDS and load balancing improve detection and distribution but may struggle under massive or sophisticated attacks. SDN and ML-based methods offer high responsiveness and intelligence but come at the cost of higher resource consumption and implementation complexity. Therefore, a hybrid approach that integrates multiple strategies tailored to the specific needs and capabilities of a cloud environment is often the most effective defense against diverse and evolving DDoS threats.

3.3 Recommendations for Improved Security Posture in Cloud Systems

First and foremost, cloud service providers and users should implement a layered defense strategy, often referred to as defense-in-depth. This involves combining multiple security controls across different layers of the systemnetwork, application, and user interface(Kuipers & Fabro, 2006). By integrating firewalls, intrusion detection and prevention systems (IDPS), web application firewalls (WAFs), and rate-limiting tools, organizations can reduce their reliance on any single mechanism and significantly improve their ability to resist various forms of DDoS attacks.

Second, organizations should leverage real-time monitoring and anomaly detection systems, ideally powered by machine learning algorithms. These systems can learn traffic patterns over time and identify deviations that indicate potential DDoS activity. Unlike static rule-based systems, ML-based models offer adaptability and can detect novel or stealthy attacks that traditional filters may overlook. It is also advisable to integrate these systems with automated incident response protocols to ensure rapid action once an attack is detected.

Another important recommendation is to adopt Software-Defined Networking (SDN) and Network Function Virtualization (NFV)(Papavassiliou, 2020). These technologies provide enhanced control and flexibility in managing network traffic, allowing for dynamic rerouting, throttling, or blackholing of malicious traffic without affecting legitimate users. SDN can also assist in isolating affected network segments to contain the spread of the attack.

Moreover, cloud environments should ensure the proper configuration and hardening of APIs and exposed services, as these are common targets in DDoS and application-layer attacks. This includes implementing authentication and authorization controls, rate-limiting access to APIs, and conducting regular security audits to detect and patch vulnerabilities.

Organizations should also establish collaborative threat intelligence sharing practices(Brown et al., 2015). By participating in threat intelligence networks and sharing information on attack signatures, IP blacklists, and emerging tactics, cloud service providers and users can enhance their collective defense and reduce response times. In this regard, standardized platforms for real-time data exchange between cloud tenants, providers, and cybersecurity agencies are essential.

Furthermore, cloud users must be aware of economic vulnerabilities, such as those exploited in Economic Denial of Sustainability (EDoS) attacks. To address this, it is advisable to set usage thresholds and cost-monitoring alerts, preventing uncontrolled resource consumption triggered by prolonged low-volume attacks.

Finally, a comprehensive incident response and recovery plan should be developed and regularly tested. This includes not only technical response protocols but also communication strategies, data backup procedures, and business continuity planning. Educating staff and stakeholders about DDoS threats and response roles can further enhance organizational preparedness.

Improving the security posture of cloud systems against DDoS attacks requires a combination of proactive defense mechanisms, intelligent detection systems, architectural improvements, and cross-organizational collaboration. By adopting a holistic and adaptive approach, cloud environments can better withstand the increasing frequency and sophistication of DDoS threats.

3.4 Implications and Contributions

From a practical perspective, the research offers actionable insights for cloud service providers, enterprise IT teams, and security professionals(Dutta et al., 2013). By identifying the most commonly exploited vulnerabilities such as exposed APIs, overloaded load balancers, and the economic impact of autoscaling this study helps stakeholders prioritize their defensive measures and allocate resources more effectively. The comparative evaluation of mitigation techniques, including traditional methods, SDN-based approaches, and machine learning-driven detection models, provides a foundation for informed decision-making when designing or upgrading security architectures.

Additionally, this study emphasizes the importance of hybrid defense strategies that integrate multiple layers of protection and adapt to the dynamic nature of cloud environments. This finding may influence how organizations approach cloud security by encouraging them to move beyond singular, static solutions and instead adopt more flexible, intelligence-driven frameworks. The insights into the limitations of existing commercial DDoS protection tools also guide smaller businesses and institutions in selecting or developing affordable, scalable solutions that meet their specific needs.

In terms of academic contribution, this research adds to the body of knowledge in cloud security by bridging a gap between theoretical vulnerability assessment and applied mitigation performance testing(Khorshed et al., 2012). Unlike prior studies that often focus solely on one aspect either attack classification or a specific defense mechanism this study offers a comprehensive analysis that spans identification, simulation, and performance comparison. The methodology combining real-world simulation tools, threat modeling, and statistical analysis can serve as a reference for future studies aiming to evaluate security frameworks in virtualized environments.

Furthermore, the research highlights the emerging potential of technologies such as Software-Defined Networking (SDN) and machine learning in fortifying cloud defenses. These findings can inspire further research into the optimization of AI models for real-time DDoS detection or the development of SDN protocols specifically tailored to cloud security. It also opens the door for multidisciplinary collaboration, involving experts in networking, artificial intelligence, and cloud architecture.

The implications of this research extend beyond technical solutions; they also underscore the strategic importance of proactive, intelligent security planning in a digital age dominated by cloud computing(Conti et al., 2012). The contributions made by this study are expected to not only enhance current defensive capabilities but also shape future innovations in safeguarding cloud systems from DDoS threats.

4. CONCLUSION

As cloud computing continues to evolve into a foundational technology for modern digital infrastructure, securing cloud systems against Distributed Denial of Service (DDoS) attacks has become more critical than ever. This research set out to analyze the vulnerabilities inherent in cloud environments and evaluate the effectiveness of various mitigation strategies designed to counter DDoS threats. The findings underscore the complex and evolving nature of DDoS attacks and reveal that cloud infrastructures, due to their shared resource model, open interfaces, and elastic architecture, present unique challenges for defense. Through systematic vulnerability analysis, the study identified several key areas that attackers frequently exploit, including unsecured APIs, auto-scaling mechanisms, and overburdened load balancers. These weak points, if not properly managed, can lead to widespread service disruption, economic damage, and loss of user trust. By simulating various types of DDoS attacks in a controlled environment and applying multiple mitigation strategies ranging from traditional methods like rate limiting to more advanced approaches like Software-Defined Networking (SDN) and machine learning-based detection the research was able to highlight the strengths and limitations of each approach. The performance comparison revealed that while conventional tools remain useful for mitigating low-complexity attacks, they are often inadequate against large-scale or sophisticated threats. On the other hand, SDN and AI-driven techniques demonstrated superior adaptability and responsiveness, though they require significant resources and expertise to implement effectively. This highlights the need for a balanced, hybrid defense strategy that can provide comprehensive protection across different attack surfaces. In light of these findings, the research offers practical recommendations for improving cloud security, such as adopting layered defense models, enhancing traffic monitoring with intelligent detection systems, and establishing collaborative threat intelligence networks. These measures not only strengthen an organization's immediate defenses but also contribute to long-term resilience against evolving cyber threats. This study contributes valuable insights to both academic and practical domains, emphasizing the urgent need for adaptive, scalable, and proactive security frameworks in cloud computing. By addressing the dual aspects of vulnerability analysis and mitigation performance, this research lays a foundation for further exploration and innovation in cloud-based cybersecurity strategies, ultimately helping organizations safeguard their digital assets in an increasingly interconnected world.

REFERENCES

Agrawal, N., & Tapaswi, S. (2019). Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. *IEEE Communications Surveys & Tutorials*, *21*(4), 3769–3795.

Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. *Internet of Things*, *12*, 100273.

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, 43–49.

Chalvatzis, I., Karras, D., & Papademetriou, R. (2020). Reproducible modelling and simulating security vulnerability scanners evaluation framework towards risk management assessment of small and medium enterprises business networks. *Indian Journal of Science and Technology*, *13*(37), 3910–3943.

Conti, M., Das, S. K., Bisdikian, C., Kumar, M., Ni, L. M., Passarella, A., Roussos, G., Tröster, G., Tsudik, G., & Zambonelli, F. (2012). Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. *Pervasive and Mobile Computing*, *8*(1), 2–21.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*, *44*(5), 643–666.

Downing, S. M. (2004). Reliability: on the reproducibility of assessment data. *Medical Education*, *38*(9), 1006–1012.

Dutta, A., Peng, G. C. A., & Choudhary, A. (2013). Risks in enterprise cloud computing: the perspective of IT experts. *Journal of Computer Information Systems*, *53*(4), 39–48.

Gebreyes, A. (2020). *Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues*. Walden University.

Gupta, B. B., & Dahiya, A. (2021). *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC press.

Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., & Choo, K.-K. R. (2016). On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. *Journal of Network and*

Computer Applications, *74*, 98–120.
Jayakumar, S. (2020). Cyber attacks by terrorists and other malevolent actors: Prevention and preparedness with three case studies on Estonia, Singapore, and the United States. *Handbook of Terrorism Prevention and Preparedness*, 871–925.
Kaul, D., & Khurana, R. (2021). AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. *Eigenpub Review of Science and Technology*, *5*(1), 34–62.
Khorshed, M. T., Ali, A. B. M. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, *28*(6), 833–851.
Kufakunesu, R., Hancke, G. P., & Abu-Mahfouz, A. M. (2020). A survey on adaptive data rate optimization in lorawan: Recent solutions and major challenges. *Sensors*, *20*(18), 5044.
Kuipers, D., & Fabro, M. (2006). *Control systems cyber security: Defense in depth strategies*. Idaho National Lab.(INL), Idaho Falls, ID (United States).
Murphy, B. R. (2019). *Comparing the performance of intrusion detection systems: Snort and Suricata*. Colorado Technical University.
Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. *Ieee Access*, *9*, 78658–78700.
Okolo, F. C., Etukudoh, E. A., Ogunwole, O., Osho, G. O., & Basiru, J. O. (2021). Systematic review of cyber threats and resilience strategies across global supply chains and transportation networks. *Journal Name Missing*.
Papavassiliou, S. (2020). Software defined networking (SDN) and network function virtualization (NFV). In *Future Internet* (Vol. 12, Issue 1, p. 7). MDPI.
Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, *76*, 5320–5363.
Sharma, H. (2020). Effectiveness of CSPM in Multi-Cloud Environments: A study on the challenges and strategies for implementing CSPM across multiple cloud service providers (AWS, Azure, Google Cloud), focusing on interoperability and comprehensive visibility. *International Journal of Computer Science and Engineering Research and Development (IJCSERD)*, *10*(1), 1–18.
Sivetc, L., Wijermars, M., & Lehtisaari, K. (2019). *The blacklisting mechanism*. Routledge Abingdon, UK.
Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet Computing: Principles of Distributed Systems and Emerging Internet-Based Technologies*, 195–236.
Verma, S., & Bala, A. (2021). Auto-scaling techniques for IoT-based cloud applications: a review. *Cluster Computing*, *24*(3), 2425–2459.
Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2015). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, *18*(1), 602–622.