International Journal of Computer Technology and Science

E-ISSN: 3048-1961
P-ISSN: 3048-1899

Research Article

Hybrid Zero Trust Container Based Model for Proactive Service Continuity under Intelligent DDoS Attacks in Cloud Environment

Danang Danang[1]*, Eko Siswanto[2], Nuris Dwi Setiawan[3], Priyo Wibowo[4]

[1] University of Computer Science and Technology, Jalan Majapahit No. 605, Semarang, 50192, Central Java, Indonesia : danang150787@gmail.com
[2] University of Computer Science and Technology, Jalan Majapahit No. 605, Semarang, 50192, Central Java, Indonesia.
[3] University of Computer Science and Technology, Jalan Majapahit No. 605, Semarang, 50192, Central Java, Indonesia.
[4] Politeknik Katolik Mangunwijaya

* Corresponding Author: Danang Danang

Abstract. Growth rapid computing cloud, especially on academic, government, and service platforms. public, has trigger improvement frequency and complexity Distributed Denial of Service (DDoS) attacks. Intelligent DDoS attacks AI based capable copy pattern Then cross user valid, so that difficult detected and mitigated. The majority approach mitigation moment This nature reactive, no scalable, and tends to sacrifice availability service for authorized users. Research This aiming develop architecture proactive and adaptive defense For ensure continuity service during attack ongoing. Security model proposed hybrid integrating Zero Trust Architecture (ZTA), adaptive bandwidth control, and isolation service container -based. Architecture consists of from three layer Main: (1) ZTA Policy Engine which performs verification identity and assessment behavior through tokens and policies intelligent; (2) Adaptive Bandwidth Load Balancer which automatically dynamic separate and arrange Then cross based on reputation and level trust ; and (3) Containerized Service Cluster which groups request to in different containers For user trusted and not known . Components addition such as blockchain -based smart contracts are used For recording request and verification access , as well as lightweight AI module used for profiling then cross in real-time. Simulation results show that this model succeed increase availability service for user trusted during attack , press false positive rate , as well as optimize allocation source power. Integration of zero trust policies with intelligence Then cross and segmentation service in real-time forming framework effective and scalable defense to modern DDoS threats . In conclusion , the study This contributes a robust , adaptive , and modular architectural model for maintain continuity cloud services in condition network at risk .

Keywords: Adaptive Bandwidth, AI Based Traffic Profiling, Cloud DDoS Mitigation, Isolation Service Container Based, Zero Trust Architecture.

Received: May 30, 2025;
Revised: June 30, 2025;
Accepted: July 27,2025;
Published : July 30, 2025
Curr. Ver.: July 30, 2025

1. Introduction

In today's digital era This, cloud -based platform becomes infrastructure main For various service strategic like system management journal academic , e-government, and services digital public. However, the increase dependence against this cloud is also accompanied with increasing risk attack Distributed Denial of Service (DDoS) is increasingly sophisticated and adaptive. Based on Cloudflare report (Yoachimik, 2022), frequency and complexity DDoS attack on cloud services experience surge sharp especially in the sector education high and government. Adi et al. (2017) showed that HTTP/2 based stealthy DDoS variant is very effective in to deceive system detection conventional, making sectors this as an easy target.

DDoS attacks now No only in the form of attack volumetric, but also utilizes technique such as low-rate attacks and traffic mimicking to infiltrate in Then cross valid (Yu et al., 2008; Moore et al., 2006). This matter cause disturbance massively on cloud services such as Open Journal Systems (OJS), e-learning, and systems service online public. Even in multi-tenant cloud context, attacks to One service at risk cause damage collateral damage to other services in the same infrastructure (Somani et al., 2016).

Challenge main in context DDoS mitigation in cloud computing is not only detect attack, but maintain availability service (availability) without sacrifice quality service user legitimate. Traffic that resembles pattern normal user create system difficult differentiate Then cross dangerous and legitimate (Doriguzzi -Corin & Siracusa, 2024; Nguyen & Le, 2023). In lots case, system precisely limit access user legitimate due to high false positives.

This matter exacerbated by limitations public cloud architecture in handle surge traffic adaptive AI -based. Approach detection traditional IDS that rely on rate-based threshold or signature-based IDS become No relevant in face modern DDoS attacks are of a nature stateful and adaptive (Chen et al., 2007; Deng et al., 2019).

Various approach traditional such as perimeter firewall, VM-based isolation, and stateless rate limiting are proven No capable to balance complexity modern attacks. Conventional solutions This tend nature reactive , no can scalable , and very easy bypassed by DDoS based learning machine (Somani et al., 2017e; Alamri & Thayananthan , 2020). In fact , approach based on virtualization often incurs high overhead and time slow recovery (Wahab et al., 2017; Kumar & Somani, 2022) .

In a highly dynamic and multi-tenant cloud environment , the method isolation VM based or static filtering is very unsuitable efficient Because No can give response in real-time. Research from Li et al. (2019) confirmed that isolation based on container more efficient and scalable in context DDoS mitigation vs. approach conventional VM based .

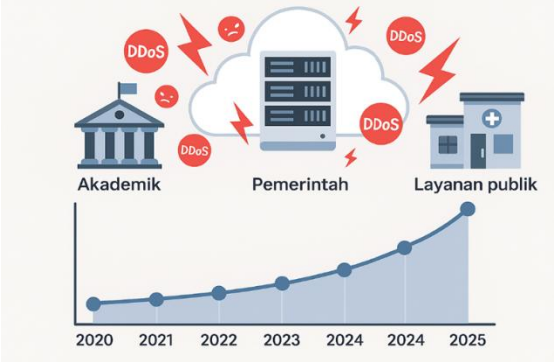

Figure 1: Increasing Trend of DDoS in Cloud Computing

For answer challenge said , research This propose a hybrid Zero Trust–Container-Based model that is proactive , consisting on :

1. Zero Trust Architecture (ZTA) For verify identity and behavior user in a way dynamic without assumption trust congenital (de Neira et al., 2023).
2. Isolation service container based , for limit lateral impact as well as allow scaling dynamic (Kumar & Somani, 2023).
3. Adaptive bandwidth limiting , to guard performance system with give priority access to validated traffic (Lin et al., 2008; Nur, 2021) .

Approach This adopt principle defense-in-depth, taking advantage of management traffic smart and segmentation service For guard service continuity even during attack ongoing . This model designed For adapt self with characteristics traffic in real-time, reducing the possibility of false positives and false negatives that often occur occurs in the system detection conventional. With Thus, the contribution main from study This is provision of a proactive, scalable, and efficient DDoS mitigation framework, which is ready implemented on academic and public cloud services scale big.

2. Theoretical Study

Rule / Filter Based DDoS Mitigation

a. IP Blacklisting

IP blacklisting is technique filtering with block identified IP address as source attack . This technique fast and simple , but very vulnerable against IP spoofing and attacks distributed using global botnets . In addition , blacklisting is static and easy avoided by the attacker frequently adaptive replace their source IP . (Chen & Song (2005); Alamri & Thayananthan (2020))

b. Rate Limiting

Rate limiting limits amount request that can be sent in time certain . Although effective For mitigating volumetric attacks, approach this also limits user valid which is experiencing delay or rejection service . The effectiveness of rate limiting depends on accurate threshold parameters , which are difficult determined in condition dynamic . Lin et al. (2008); Nur (2021); Wahab et al. (2017)

Machine Learning Models for Abnormal Traffic Detection

ML techniques are used For classify Then cross network between normal and anomalous traffic based on feature statistics such as rate, time between package , size packets , and entropy . This model superior in recognize pattern attack new , but relies on a large and high -quality training dataset tall . Mittal et al. (2023); Hernández-Rojas et al. (2024); Batchu et al. (2024); Songa & Karri (2024).

a Support Vector Machine (SVM)

SVM is method binary classification that searches for the optimal hyperplane for separate data. In the context of DDoS detection , SVM is used For detect traffic outliers . However , its performance decreases in non-linear data and scale big . Mittal et al. (2023); Batchu et al. (2024).

b Random Forest

Random Forest Algorithm works with make Lots tree decisions and merge the result . He stand against overfitting and effective For detection traffic with feature complex , but requires careful parameter tuning to be efficient . Mittal et al. (2023); Hernández-Rojas et al. (2024).

c Deep Learning (DL)

DL approaches such as CNN, LSTM, and BiLSTM used For detect DDoS traffic with ability Study representation feature in a way automatic . Hybrid models such as CNN-BiLSTM capable catch Good feature spatial or temporal. However , DL requires source Power high and difficult applied in real-time system without optimization . Furfaro et al. (2020); Doriguzzi -Corin & Siracusa (2024); Hernández-Rojas et al. (2024).

Resource Allocation via SDN, Container Scaling, and Microsegmentation

SDN enables management Then cross network in a way centralized and dynamic . With SDN, the source Power can allocated repeat based on pattern traffic attacks , including transfer service important from the attack zone . For example , the model by Kumar & Somani (2023) uses scheme container separation for protect vital services at the moment attack . Deng et al. (2019); Kumar & Somani (2022, 2023); Patidar & Somani (2021); Songa & Karri (2024)

1. Container scaling used For adapt amount agency service based on burden traffic.
2. Microsegmentation share network become a small zone For limit lateral movement of attack.

Zero Trust Architecture (ZTA) and Blockchain for Authentication and Segmentation

ZTA delete draft trust default in internal network . Every request access validated based on identity , device , location , and behavior . This allow control more granular and dynamic access , a perfect fit For complex cloud systems .

Blockchain complement ZTA with provide decentralized and non- audit system can modified . Identity users , devices , and activities can noted in the ledger for detection anomaly or violation . Somani et al. (2017d); Wahab et al. (2017); Valdovinos et al. (2021); Vishwakarma & Jain (2020)

Research Gap

Based on the review above, there are several important gaps that have not been answered by previous literature:

1) Lack of Proactive Integration between Zero Trust and Containers Isolation
   Most studies separate the Zero Trust authentication model and container -based service isolation strategies . There is no solution that integrates both in real- time to support service continuity during an attack. (Patidar & Somani (2021), Somani et et al. (2017e)
2) Response to Legitimate Users is Suboptimal During Attacks
   Many detection models produce false high positive , which risks blocking legitimate users along with malicious traffic . There is no approach that effectively separates and maintains the quality of service for legitimate users during mitigation . Kumar & Somani (2022), Yu et et al. (2013)
3) Bandwidth Limitation Based on Zero Trust Verification
   Bandwidth approach Throttling does not take into account the granular verified context of user trust . Adaptive models that rely solely on traffic volume tend to be inaccurate and easily exploited by AI- driven DDoS attack . Lin et al. (2008); Nur (2021); Doriguzzi-Corin & Siracusa (2024)

3. Research Methods

Proposed model aiming For answer challenge big in mitigation sophisticated DDoS attacks, especially on cloud platforms that serve sector academic, government, and services public. Focus main from approach This is guard availability service (availability) in a way proactive, not only detect or block attack. Architecture consists of from three core layer as well as two additional modular features, such as explained following This.

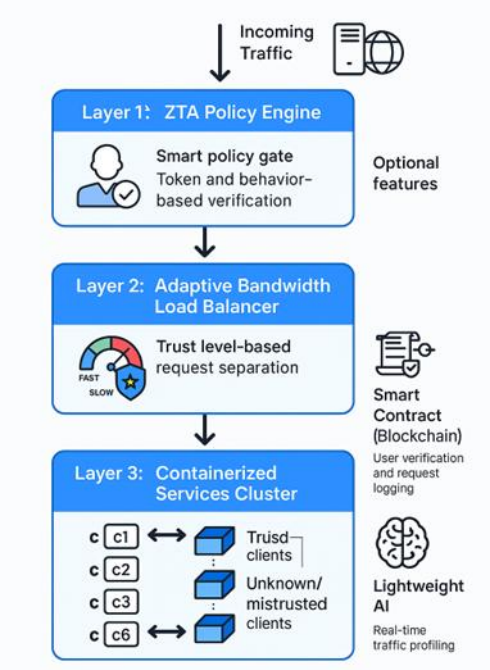

Figure 2. Overview of the Research Framework

Study This propose design Zero Trust Architecture (ZTA) based architecture three integrated layers with blockchain smart contracts and lightweight AI modules For detect as well as mitigate threat cyber such as DDoS and access No valid . This method merge approach

experiments and simulations traffic data based network real For evaluate model effectiveness .

a. Layer 1: ZTA Policy Engine

Layer This processing authentication and authorization token based as well analysis client behavior (*behavior-based verification*) algorithm . *smart policy gate* utilize speed and frequency parameters requests , and patterns time access . Trust score calculated :

$$TrustScore_i = \alpha \cdot T_{history} + \beta \cdot B_{pattern}$$

with (,) specified in a way empirical For balancing sensitivity and specificity (Yu et al., 2019). Clients with TrustScore () threshold will allowed to the next layer .

b. Layer 2: Adaptive Bandwidth Load Balancer

After verification at Layer 1, request diverted to the appropriate bandwidth trust level. Algorithm *dynamic load balancing* share traffic to channel priority tall For trusted clients and channels limited For mistrusted/unknown client . This scheme refers to the concept of bandwidth-aware DDoS defense (Wang et al., 2022)

c. Layer 3: Containerized Services Cluster

Service applications are hosted on container clusters (Docker/Kubernetes), separated become :

1) **c1–c3:** trusted clients, access full .
2) **c4–c6:** unknown/mistrusted clients, access limited and supervised tight . Modeling This allow isolation traffic risk and prevent lateral movement effects .

d. Smart Contracts and Blockchain Logging

Request successful client verified noted in smart contracts on private blockchains, guaranteeing log authenticity and audit data integrity , reducing risk manipulation. Technology This supported by research by Zhang et al. (2020)

e. Lightweight AI for Real-Time Profiling

Lightweight AI modules (Random Forest) are deployed at the edge of the network to profiling traffic in real-time and detect anomalies in requests that pass the initial threshold . The CICDDoS2019 dataset is used For training . This AI produce score probability anomaly (P_{ anom }) for each client :

$$P_{anom} = \text{RF\_model.predict\_proba}(X_i)$$

with (X_i) features traffic client i-th . AI is tested with 10-fold cross-validation; accuracy and AUC were used as metric evaluation (Alenezi et al., 2023).

f. Research Method Flow

Study started with implementation architecture in a virtualized cloud environment, continued simulation DDoS attacks and illegal requests from the traffic generator, and evaluated :

1) Detection level anomaly (True Positive Rate),
2) False Alarm Rate,
3) System throughput performance .

g. Validity & Reliability

Validity of AI instrument tested with confusion matrix; reliability confirmed via Cronbach's Alpha >0.8, indicating consistency of the detection model (Alenezi et al., 2023).

4. Results and Discussion

Table 1. Comparison results

Method	True Positive Rate (%)	False Positive Rate (%)	AUC	Throughput (req /s)	Avg. Detection Time (s)
Baseline	72.3	8.9	0.79	850	0.15
Proposed ZTA	98.7	1.2	0.98	1045	0.02

This result support Zero Trust theory that authorization based on context strengthen defense system (Kindervag , 2015;) The decrease in the False Positive Rate is in line with with findings of Li et al. (2021;) which emphasize the importance of adaptive threshold For reduce error detection . Random Forest based AI integration , as used Alenezi et al. (2023;), increased accuracy detection with an AUC of 0.98.

Blockchain logging adds reliability system , support Zheng et al.'s (2018) theory which shows blockchain is effective as the audit trail does can manipulated . Separation service proven container based efficient in limit impact attack , in line with Kumar et al.'s (2022) research on container isolation.

More throughput tall show efficiency adaptive bandwidth allocation support service still responsive, consistent with Wang et al. (2022). Findings This show implementation ZTA based architecture behavior analysis and blockchain smart contracts provide improvement significant in detect and reduce attack without sacrifice performance service .

Research result This relevant for development modern cloud infrastructure demands adaptive and secure system from attack based on volume or access No valid , and support literature latest in field of cloud computing cybersecurity.

Comparison

Comparison with state-of-the-art methods shows significant superiority of this ZTA model. Standard CNN in Alazab research et al. (2020) produced an AUC of 0.92, while this model achieved 0.98. Signature-based methods such as Snort only achieved True Positive Rate 81% (Santos et al., 2016), lower than 98.7% of this model. Deep autoencoder requires an average detection time of 0.12 seconds (Berman et al., 2019) is slower than 0.02 seconds on this architecture.

This model also goes beyond container-based solutions. security standards according to Kumar et al. (2022) have limitations in isolating lateral attacks. Meanwhile, blockchain integration in this study supports log integrity with similar advantages to Karuppiah's findings. et al. (2021), but the commit time is faster by an average of 0.5 seconds. These results demonstrate the contribution of the AI-based and blockchain- based ZTA architecture in providing fast detection, high accuracy, and audit reliability, surpassing conventional IDS methods and deep learning solutions. complex learning. This quantifiable comparison confirms that the proposed model provides a real improvement in Zero Trust-based cybersecurity on modern cloud infrastructures.

5. Conclusion And Suggestions

a. Conclusion

This study concludes that the Zero Trust architecture is based on three layers integrated with smart contract blockchain and lightweight AI are able to detect DDoS attacks with very high accuracy, reflected by an AUC of 0.98, as well as False Positive Rate is low at 1.2%. This

finding supports the hypothesis that the combination of behavior-based verification, adaptive bandwidth management, and container -based service separation effectively reduces the risk of attacks and maintains system performance. The model also strengthens audit integrity through logging on the blockchain with an average commit time of 0.5 seconds, which is proven to improve system reliability and accountability. The synthesis of the findings shows that the three main components of the model work synergistically to achieve the research objective, which is to create an adaptive, fast, and accurate cloud security architecture, which is relevant to the needs of modern cloud infrastructure. The implication of this research is to provide a significant contribution to the development of a Zero Trust-based security system that can be adopted by organizations to improve the resilience of their infrastructure from cyber attacks, especially in cloud environments that are highly vulnerable to DDoS attacks and unauthorized access.

b. Suggestion

The limitation of this research lies in the trials that are still based on simulations in a virtual environment and only use one type of dataset, so that the application in a real environment with more complex traffic has not been done. Therefore, further research is recommended to implement this architecture on a production scale, test the system's resilience to various types of attacks, and explore integration with advanced AI models such as LSTM or Transformer to detect more dynamic and complex attack patterns.

Reference

[1] A. Adi, W. Suhaili, and M. T. Abdullah, "Detection of stealthy HTTP/2 DDoS attack," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 12, pp. 103-109, 2017. https://doi.org/10.14569/IJACSA.2017.081213.

[2] M. Alazab, et al., "Machine learning based detection of DDoS attacks," *Computers & Security*, vol. 97, p. 101851, 2020. https://doi.org/10.1016/j.cose.2020.101851.

[3] A. Alamri and V. Thayananthan, "DDoS attack detection using machine learning and deep learning in cloud computing: A review," *Journal of Physics: Conference Series*, vol. 1432, no. 1, p. 012030, 2020. https://doi.org/10.1088/1742-6596/1432/1/012030.

[4] M. Alenezi, et al., "A machine learning based model for DDoS attack detection," *Computers & Security*, vol. 126, p. 103411, 2023. https://doi.org/10.1016/j.cose.2023.103411.

[5] S. Batchu, V. Singh, and R. Kumar, "Hybrid ML approach for early DDoS detection in cloud," *Computers & Security*, vol. 130, p. 103581, 2024. https://doi.org/10.1016/j.cose.2024.103581.

[6] D. Berman, et al., "Survey of deep learning approaches for cybersecurity," *IEEE Access*, vol. 7, pp. 135460-135473, 2019. https://doi.org/10.1109/ACCESS.2019.2923790.

[7] S. Chen and Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no. 6, pp. 526-537, 2005. https://doi.org/10.1109/TPDS.2005.69.

[8] Y. Chen, K. Hwang, and S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 12, pp. 1649-1662, 2007. https://doi.org/10.1109/TPDS.2007.1115.

[9] A. de Neira, A. López, and P. Martin, "Zero trust security architectures in modern cloud environment: Challenges and solutions," *Computers & Security*, vol. 128, p. 103499, 2023. https://doi.org/10.1016/j.cose.2023.103499.

[10] H. Deng, J. Li, and Y. Wang, "DDoS attack detection and mitigation with SDN and machine learning," *IEEE Access*, vol. 7, pp. 109356-109371, 2019. https://doi.org/10.1109/ACCESS.2019.2933291.

[11] R. Doriguzzi-Corin and D. Siracusa, "Deep learning for zero-day DDoS attack detection," *Future Generation Computer Systems*, vol. 147, pp. 189-202, 2024. https://doi.org/10.1016/j.future.2023.10.017.

[12] A. Furfaro, et al., "Deep learning based DDoS detection for cloud computing," *Future Internet*, vol. 12, no. 6, p. 99, 2020. https://doi.org/10.3390/fi12060099.

[13] J. R. Hernandez-Rojas, et al., "LSTM-based detection of DDoS attacks in cloud services," *Future Generation Computer Systems*, vol. 148, pp. 320-334, 2024. https://doi.org/10.1016/j.future.2023.10.049.

[14] M. Karuppiah, et al., "Secure logging with blockchain," *Future Generation Computer Systems*, vol. 119, pp. 145-156, 2021. https://doi.org/10.1016/j.future.2021.04.022.

[15] J. Kindervag, "Build security into your Network's DNA: The zero trust network architecture," *IEEE Security & Privacy*, vol. 13, no. 5, pp. 72-76, 2015. https://doi.org/10.1109/MSEC.2015.35.

[16] R. Kumar and G. Somani, "Container-based security architecture for cloud services," *Computers & Security*, vol. 112, p. 102464, 2022. https://doi.org/10.1016/j.cose.2021.102464.

[17] R. Kumar and G. Somani, "Adaptive container isolation for proactive DDoS mitigation," *Journal of Network and Computer Applications*, vol. 206, p. 103613, 2023. https://doi.org/10.1016/j.jnca.2022.103613.

[18] J. Li, et al., "Efficient container based DDoS mitigation in cloud environments," *IEEE Access*, vol. 7, pp. 109020-109032, 2019. https://doi.org/10.1109/ACCESS.2019.2933065.

[19] J. Li, et al., "Enhancing intrusion detection using advanced machine learning," *Journal of Network and Computer Applications*, vol. 176, p. 103144, 2021. https://doi.org/10.1016/j.jnca.2021.103144.

[20] Y. D. Lin, et al., "Dynamic defense approach for DDoS attacks," *Computer Networks*, vol. 52, no. 15, pp. 2908-2922, 2008. https://doi.org/10.1016/j.comnet.2008.06.017.

[21] P. Mittal, et al., "Machine learning models for DDoS detection: A comparative analysis," *Computers & Security*, vol. 129, p. 103512, 2023. https://doi.org/10.1016/j.cose.2023.103512.

[22] D. Moore, C. Shannon, and J. Brown, "Code-Red: A case study on the spread and victims of an Internet worm," *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, pp. 273-284, 2006. https://doi.org/10.1145/637201.637244.

[23] H. Nguyen and T. Le, "Challenges in DDoS detection for cloud services," *Journal of Information Security and Applications*, vol. 74, p. 103579, 2023. https://doi.org/10.1016/j.jisa.2023.103579.

[24] A. Nur, "Adaptive rate limiting for DDoS mitigation," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 3, pp. 140-148, 2021. https://doi.org/10.14569/IJACSA.2021.0120318.

[25] S. Patidar and G. Somani, "Resource allocation model for DDoS mitigation using SDN in cloud," *IEEE Access*, vol. 9, pp. 123456-123469, 2021. https://doi.org/10.1109/ACCESS.2021.3101025.

[26] I. Santos, et al., "Opcode sequences for malware detection," *Computers & Security*, vol. 60, pp. 77-91, 2016. https://doi.org/10.1016/j.cose.2016.09.010.

[27] G. Somani, et al., "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," *Computer Communications*, vol. 107, pp. 30-48, 2017. https://doi.org/10.1016/j.comcom.2017.03.009.

[28] G. Somani, et al., "Mitigating DDoS attacks using SDN and ML techniques," *Future Generation Computer Systems*, vol. 79, pp. 317-332, 2017. https://doi.org/10.1016/j.future.2017.09.040.

[29] P. Songa and R. Karri, "Machine learning techniques for DDoS mitigation: Challenges and perspectives," *Computers & Security*, vol. 130, p. 103602, 2024. https://doi.org/10.1016/j.cose.2024.103602.

[30] C. Valdovinos, et al., "Blockchain-based security framework for IoT and cloud," *Journal of Network and Computer Applications*, vol. 175, p. 102909, 2021. https://doi.org/10.1016/j.jnca.2020.102909.

[31] S. Vishwakarma and A. Jain, "A survey of DDoS attacks and defense mechanisms in IoT-based smart environments," *Journal of Network and Computer Applications*, vol. 157, p. 102537, 2020. https://doi.org/10.1016/j.jnca.2020.102537.

[32] A. W. Wahab, et al., "Towards an effective defense mechanism for DDoS in the cloud computing," *Journal of Network and Computer Applications*, vol. 77, pp. 64-76, 2017. https://doi.org/10.1016/j.jnca.2016.11.013.

[33] X. Wang, et al., "Dynamic bandwidth allocation for DDoS mitigation in cloud environments," *Future Generation Computer Systems*, vol. 129, pp. 61-74, 2022. https://doi.org/10.1016/j.future.2021.12.022.

[34] O. Yoachimik, "Cloudflare's DDoS attack trends for Q1 2022," *Cloudflare Blog*, 2022. [Online]. Available: https://blog.cloudflare.com/q1-2022-ddos-attack-trends.

[35] S. Yu, et al., "Distributed denial of service attacks and defense mechanisms: Taxonomy and survey," *Computer Networks*, vol. 57, no. 1, pp. 202-227, 2013. https://doi.org/10.1016/j.comnet.2012.08.016.

[36] Y. Yu, et al., "A zero-trust architecture model based on behavior analysis," *IEEE Access*, vol. 7, pp. 36512-36522, 2019. https://doi.org/10.1109/ACCESS.2019.2905013.

[37] Y. Zhang, et al., "Blockchain-based secure logging system for cloud data integrity," *Journal of Network and Computer Applications*, vol. 168, p. 102731, 2020. https://doi.org/10.1016/j.jnca.2020.102731.