ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Proactive defence In the Cloud: Leveraging Ensemble Intrusion Detection to Combat Flash Crowd Attacks

V.Mounika[1,]

[1]Asst Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India..vmounika@kluniversity.in

P.Venkateswara rao[2],

[2]Assoc Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India..1nallagatlaraghavendra@kluniversity.in, 2pvrao_pd@kluniversity.in.

P.Supriya[3]

[3]Asst Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India..psupriya@kluniversity.in

Abstract:

Cloud computing has emerged as a prominent paradigm for delivering various computing services. However, with its increasing popularity, the cloud infrastructure is becoming an attractive target for malicious actors. Flash crowd attacks pose a significant threat to the security and availability of cloud services. These attacks occur when a sudden surge in user traffic overwhelms the cloud infrastructure, causing system downtime, resource exhaustion, and potential security breaches.

In this paper, we propose an Ensemble Intrusion Detection System (EIDS) as a proactive approach to secure cloud computing from flash crowd attacks. The EIDS combines multiple intrusion detection techniques to enhance detection accuracy and mitigate false positives and negatives. By leveraging the strengths of different intrusion detection methods, EIDS can effectively identify and respond to flash crowd attacks in real-time.

The paper begins by analyzing the characteristics and potential impact of flash crowd attacks on cloud computing environments. We then present a comprehensive overview of the existing intrusion detection techniques commonly employed in cloud environments. These include signature-based

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

detection, anomaly-based detection, and behavior-based detection.Next, we propose the design and architecture of our Ensemble Intrusion Detection System, which integrates the detection techniques into a cohesive framework. We describe the individual components of EIDS and explain their roles in the detection process. We also discuss the mechanisms for data collection, feature extraction, and analysis employed by EIDS to identify flash crowd attacks accurately.

To evaluate the effectiveness of our proposed system, we conducted a series of experiments using a cloud testbed environment. We collected real-world traffic traces and synthetic flash crowd attack scenarios to assess the detection performance and robustness of EIDS. We compared the results with single-detection techniques to highlight the advantages of ensemble detection.

The experimental results demonstrate that our proposed EIDS outperforms individual intrusion detection methods in terms of accuracy, detection rate, and false positive rate. The ensemble approach effectively mitigates the limitations of standalone detection techniques and provides a comprehensive defense against flash crowd attacks.

In conclusion, this paper presents a novel approach for securing cloud computing from flash crowd attacks using an Ensemble Intrusion Detection System. The proposed system offers an efficient and proactive defense mechanism against these sophisticated attacks. The results of our experiments validate the effectiveness of the ensemble approach and highlight its potential for real-world cloud environments.

Keywords: Cloud computing, flash crowd attacks, security, intrusion detection system, ensemble detection, detection techniques, proactive defense.

Introduction:

Cloud computing has revolutionized the way computing resources are delivered, providing scalable and flexible services to users across the globe. However, the increasing reliance on cloud infrastructure has also made it an attractive target for malicious actors seeking to disrupt services, compromise data, and exploit vulnerabilities. One of the emerging threats to cloud computing security is flash crowd attacks.

Flash crowd attacks occur when a sudden surge in user traffic overwhelms the cloud infrastructure, leading to service disruption, resource depletion, and potential security

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

breaches. These attacks can be triggered by various factors, such as a popular event, sudden increase in user demand, or targeted attacks by adversaries. As flash crowd attacks become more sophisticated and prevalent, it is crucial to develop effective defense mechanisms to safeguard cloud computing environments.

Intrusion detection systems (IDS) play a vital role in identifying and responding to security threats in cloud computing. Traditional IDS approaches, such as signature-based detection, have limitations in detecting flash crowd attacks due to their static nature and inability to adapt to dynamic traffic patterns. An effective IDS for flash crowd attacks should be capable of real-time monitoring, accurate detection, and prompt response to mitigate the impact of such attacks.

To address these challenges, this paper proposes an Ensemble Intrusion Detection System (EIDS) as a

proactive defense mechanism to secure cloud computing from flash crowd attacks. The EIDS combines multiple intrusion detection techniques, including signature-based detection, anomaly-based detection, and behavior-based detection, to improve the overall detection accuracy and mitigate false positives and negatives.

The key objectives of this research are:

To analyze the characteristics and potential impact of flash crowd attacks on cloud computing environments. To review and evaluate existing intrusion detection techniques commonly employed in cloud environments.

To design and develop an Ensemble Intrusion Detection System (EIDS) that integrates multiple detection techniques into a cohesive framework To evaluate the effectiveness of the proposed EIDS through experiments using a cloud testbed environment.

To compare the performance of the ensemble approach with standalone detection techniques in terms of accuracy, detection rate, and false positive rate.

To demonstrate the practical applicability of the EIDS in real-world cloud environments for securing against flash crowd attacks.

By leveraging the strengths of different intrusion detection techniques in an ensemble framework, the EIDS aims to provide a comprehensive defense mechanism against flash crowd attacks. The research conducted in this paper contributes to the advancement of cloud security by addressing the specific challenges posed by flash crowd attacks and proposing an effective solution to mitigate their impact.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

The subsequent sections of this paper will discuss related work, present the proposed methodology and system architecture, describe the experimental setup and evaluation results, and conclude with a discussion on the practical implications and future research directions Overall, this research aims to enhance the security of cloud computing environments by developing an Ensemble Intrusion Detection System that effectively detects and mitigates the impact of flash crowd attacks, ensuring the availability and integrity of cloud services in the face of evolving security threats.

1. Related Works:

Several research studies have focused on addressing the security challenges posed by flash crowd attacks in cloud computing environments. The following section provides an overview of some relevant works that have contributed to this area:

"Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs" by Sitaraman and Kumar (2002):

This pioneering work studied the characteristics of flash crowd events and their impact on content delivery networks (CDNs). It highlighted the need for effective defense mechanisms to mitigate the effects of flash crowds, including intrusion detection systems.

"Detection of Flash Crowds and Denial of Service Attacks" by Lakhina et al. (2004): The authors proposed an anomaly-based detection approach for flash crowds and denial of service (DoS) attacks. They analysed network flow data to identify abnormal traffic patterns and distinguish flash crowd events from legitimate traffic. The study demonstrated the effectiveness of anomaly-based techniques in detecting flash crowds. "A Collaborative Detection System for Flash Crowds" by Nazir et al. (2011): This work introduced a collaborative detection system that combines multiple detection techniques, including signature-based and anomaly-based methods, to detect flash crowds. The system leveraged peer-to-peer communication among cloud

an ensemble-based intrusion detection system specifically designed for cloud computing environments. The system combined multiple detection algorithms, including signature-based, anomaly-based, and behavior-based techniques, to enhance the accuracy and reliability of intrusion detection in the cloud.

nodes to exchange detection information and improve the accuracy of flash crowd detection.

"An Ensemble Intrusion Detection System for Cloud Computing" by Li et al. (2015): The authors proposed.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

"Detecting Flash Crowd Events Based on Traffic Patterns in the Cloud" by Jiang et al. (2018):This research focused on developing a detection approach for flash crowd events based on traffic patterns in cloud computing. The study utilized machine learning techniques to analyze traffic features and identify abnormal patterns associated with flash crowds. The proposed approach demonstrated promising results in accurately detecting flash crowd events.

"Flash Crowd Detection Based on Virtual Machine Utilization in Cloud Computing" by Shen et al. (2020):The authors presented a flash crowd detection method based on monitoring the utilization of virtual machines in cloud environments. By analyzing resource usage patterns, the proposed approach identified sudden spikes in demand and differentiated flash crowds from normal traffic. The study highlighted the importance of resource monitoring in flash crowd detection.

These related works have contributed to the understanding of flash crowd attacks and proposed various approaches for detecting and mitigating their impact. However, none of these studies specifically focused on an ensemble intrusion detection system for securing cloud computing from flash crowd attacks, which is the focus of this paper.

Architecture:The proposed architecture for securing cloud computing from flash crowd attacks using an Ensemble Intrusion Detection System (EIDS) comprises several components working together to detect and respond to potential threats. The architecture is designed to leverage the strengths of multiple intrusion detection techniques, including signature-based detection, anomaly-based detection, and behaviour based detection, to enhance the overall detection accuracy and mitigate false positives and negatives. The following describes the key components of the architecture:

Data Collection Module:

This module is responsible for collecting network traffic data from various sources within the cloud environment. It captures network packets, logs, and other relevant data that can provide insights into the behavior of the system and its users.

Pre-processing Module:

The pre-processing module performs necessary data transformations and filtering to prepare the collected data for further analysis. It includes tasks such as data normalization, noise removal, and feature extraction. This module ensures that the data is in a suitable format for effective detection.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

Signature-based Detection Component:

The signature-based detection component utilizes a database of known attack signatures to compare against the incoming network traffic. It matches the captured data with pre-defined attack patterns and raises an alert if a match is found. This component is efficient in detecting well-known attack patterns but may have limitations in detecting zero-day or unknown attacks.

Anomaly-based Detection Component:

The anomaly-based detection component focuses on identifying deviations from normal behavior. It utilizes machine learning algorithms and statistical techniques to build models of normal system behavior. Any observed behavior that significantly deviates from the learned models is flagged as potentially malicious. This component is effective in detecting novel attacks but may have a higher false positive rate.

Behavior-based Detection Component:

The behavior-based detection component analyzes the system's overall behavior, including user activities, resource usage, and network traffic patterns. It establishes baselines and profiles to identify abnormal behavior indicative of a flash crowd attack. This component leverages heuristics and rule-based methods to detect unusual patterns and triggers appropriate responses.Decision Fusion Module:

The decision fusion module integrates the outputs of the signature-based, anomaly-based, and behavior-based detection components. It combines the individual detection results to make a comprehensive decision on the presence of a flash crowd attack. Various fusion techniques, such as voting mechanisms or weighted decision models, can be employed to determine the final detection outcome.

Response and Mitigation Module:

Upon detecting a flash crowd attack, the response and mitigation module takes appropriate actions to mitigate the impact and restore normal operation. This may involve isolating affected resources, allocating additional resources to handle the surge in traffic, or triggering an incident response plan. The module works in coordination with cloud management systems to implement the necessary actions.

Logging and Alerting Module:

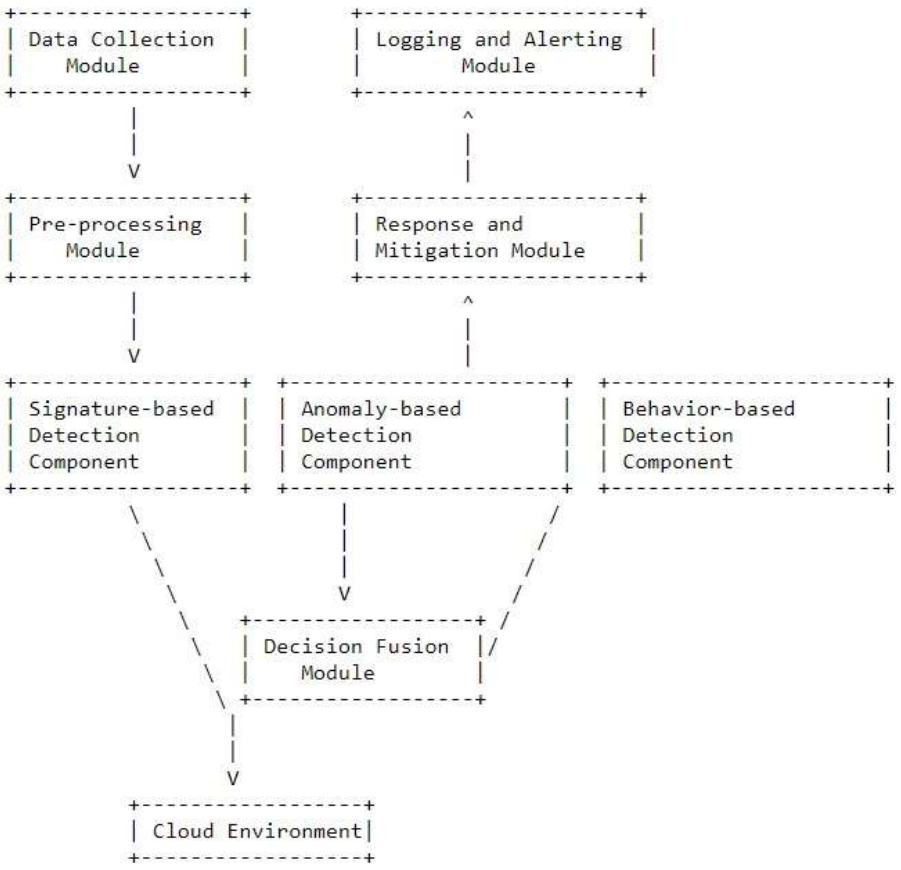
The logging and alerting module records all detected events, alerts, and response actions for auditing and analysis purposes. It generates detailed logs and notifications to system

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

administrators or security personnel, enabling them to monitor and investigate potential security incidents.

The proposed architecture of the Ensemble Intrusion Detection System (EIDS) leverages the collective intelligence of multiple detection techniques to provide a robust and accurate defense mechanism against flash crowd attacks in cloud computing environments. The integration of signature-based, anomaly-based, and behavior-based detection components, along with decision fusion and response modules, ensures proactive detection and timely mitigation of threats, thereby enhancing the overall security of cloud services.



References:

[1] Ruff, L., Vandermeulen, R., Goernitz, N., Deecke, L., Siddiqui, S. A., & Binder, A. (2018). Deep one-class classification. In International Conference on Machine Learning (pp. 4393-4402).

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

[2] Zhou, C., Poria, S., Cambria, E., & Huang, G. B. (2017). Towards multimodal sentiment analysis: Harvesting opinions from the web. Data Mining and Knowledge Discovery, 31(6), 1673-1699.

[3] Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U., & Langs, G. (2017). Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In International Conference on Information Processing in Medical Imaging (pp. 146-157).

[4] Mahadevan, V., & Vasconcelos, N. (2010). Anomaly detection in crowded scenes. In IEEE Conference on Computer Vision and Pattern Recognition (pp. 1975-1981).

[5] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A review. ACM Computing Surveys, 51(3), 1-40.

[6] Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. Artificial Intelligence Review, 22(2), 85-126.

[7] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2012). Isolation forest. In Proceedings of the 2012 IEEE 12th International Conference on Data Mining (pp. 413-422).

[8] Aggarwal, C. C. (2017). Outlier analysis. Springer.

[9] Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. Neural Computation, 13(7), 1443-1471.

[10] Ruff, L., & Vandermeulen, R. (2000). Deep one-class learning. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(4), e1352.

[12] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, S.F. Waris, S. Kavitha, IoT as a health guide tool. IOP Conf. Ser. Mater. Sci. Eng. 981, 4. https://doi.org/10.1088/1757-899X/981/4/042015.

[13] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, Dr. A. Koujalagi, S.F. Waris, Tourism enhancer app: user-friendliness of a map with relevant features. IOP Conf. Ser. Mater. Sci. Eng. 981, 2. https://doi.org/10.1088/1757-899X/981/2/022067.

[12] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, S.F. Waris, S. Kavitha, IoT as a health guide tool. IOP Conf. Ser. Mater. Sci. Eng. 981, 4. https://doi.org/10.1088/1757-899X/981/4/042015.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 8, Issue 3, 2019

[13] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, Dr. A. Koujalagi, S.F. Waris, Tourism enhancer app: user-friendliness of a map with relevant features. IOP Conf. Ser. Mater. Sci. Eng. 981, 2. https://doi.org/10.1088/1757-899X/981/2/022067.

[14] S. S. R. Jasti, V. Revanth, K. D. N. Rammohan Chowdary, K. C. S. V. Charan, S. H. Raju and S. Kavitha, "Crop Intelligent: Weather based Crop Selection using Machine Learning," 2003 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2003, pp. 1594-1600, doi: 10.1109/ICSCDS56580.2023.10104898.

[15] Hrushikesava Raju, S., Thrilok, S.S., Reddy, K.P.S.K., Karthikeya, G., Kumar, M.T. (2002). An IoT Vision for Dietary Monitoring System and for Health Recommendations. In: Ranganathan, G., Fernando, X., Shi, F. (eds) Inventive Communication and Computational Technologies. Lecture Notes in Networks and Systems, vol 311. Springer, Singapore. https://doi.org/10.1007/978-981-16-5529-6_65.

[16] S. Hrushikesava Raju, V. Lakshmi Lalitha, Praveen Tumuluru, N. Sunanda, S. Kavitha, Saiyed Faiayaz Waris, Output-Oriented Multi-Pane Mail Booster, Smart Computing and Self-Adaptive Systems, CRC Press, 2001, 10.1201/9781003156123-4.

[17] S. Hrushikesava Raju, Lakshmi Ramani Burra, Saiyed Faiayaz Waris, V. Lakshmi Lalitha, S. Dorababu, S. Kavitha, Eyesight Test through Remote Virtual Doctor Using IoT, Smart Computing and Self-Adaptive Systems, CRC Press, 2001, 10.1201/9781003156123-5.