Securing Cloud Computing Services with an Intelligent Preventive Approach

Saleh M. Altowaijri
Department of Information Systems, Faculty of Computing and Information Technology, Northern Border University, Saudi Arabia
saleh.altowaijri@nbu.edu (corresponding author)

Yamen El Touati
Department of Computer Science, Faculty of Computing and Information Technology, Northern Border University, Saudi Arabia
yamen.touati@nbu.edu.sa

Received: 15 March 2024 | Revised: 25 March 2024 | Accepted: 26 March 2024

 DOI: https://doi.org/10.48084/etasr.7268

ABSTRACT

Cloud computing is a technological marvel that transcends conventional boundaries by utilizing an Internet-based network of remote servers to store, manage, and process data and many other services. It represents a contemporary paradigm for delivering information technology services. Today, cloud computing services have become indispensable for both individuals and corporations. However, adopting cloud services presents fresh challenges in terms of service quality, resource optimization, data integration, cost governance, and operational security. The security of cloud services is of supreme importance, given the open and distributed nature of the environment, making it susceptible to various cyberattacks, such as Denial of Service (DoS) or Distributed DoS (DDoS) attacks, among others. Cyberattacks can have severe repercussions on the availability of cloud services, potentially causing complete DoS. In numerous instances, the detection of attacks is delayed, pushing cloud platforms to a breaking point. Emphasizing the importance of proactive measures, it becomes crucial to identify and alert about any suspicious access long before the latter reaches a critical stage, mitigating the risks and preventing potential service disruptions. This study introduces a preventive approach that utilizes artificial intelligence techniques to improve the security of cloud services. The proposed method aims to detect and flag potential attack behaviors well in advance before they affect service quality. To achieve this, the particular method involves periodic identification and measurement of critical information on service access and resource utilization. This can be accomplished by analyzing cloud server logs or integrating dedicated sniffing software to capture and store technical traffic details. Subsequently, the collected data are processed by analyzing traffic properties to proactively identify and report any indications of cyberattacks.

Keywords-cloud computing; cyber security; preventive approach; prediction techniques; artificial intelligence

I. INTRODUCTION

In recent years, cloud computing has emerged as a transformative force in the world of Information Technology (IT) services, offering high scalability, flexibility, and cost-effectiveness. As organizations across the globe increasingly migrate their critical data and applications to cloud environments, cybersecurity has become a pressing concern. The ever-expanding attack surface, complex network infrastructures, and the shared responsibility model present unique challenges that require vigilant and robust security measures to be taken [1]. This study combines the cloud computing domain with the cybersecurity field. These two axes are considered the pillars of recent information technology solutions. Moreover, an important step in the recommended solution is to deploy Artificial Intelligence (AI) techniques to resolve the security issues related to cloud computing.

This study aims to fortify cloud-based infrastructures against cyber incursions by meticulously scrutinizing client interaction patterns and preemptively identifying potential attack strategies [2]. This proactive approach is essential for maintaining the integrity and robustness of cloud services and ensuring that they do not succumb to operational disruptions [3]. At the core of the specific study lies the development of an innovative AI-driven method for meticulously analyzing service request data. This system is adept at flagging activities that mirror the characteristics of cyber threats, thereby safeguarding the uninterrupted availability of cloud-based solutions and fostering a secure and efficient service environment. This initiative underscores the criticality of shielding cloud platforms from malicious activities, aiming to erect a resilient defense mechanism against the ever-evolving landscape of cyber threats. The primary objective is to mitigate

DoS attacks by identifying their patterns and preventing their recurrence.

II. BACKGROUND ON SECURITY AND CYBER-ATTACKS FOR CLOUD-BASED INFRASTRUCTURES

The popularity of cloud-based infrastructures has risen due to their scale capacity, cost-effectiveness, and flexibility. Nevertheless, they also provide distinctive security obstacles and are vulnerable to diverse cyber-attacks.

A. Denial of Service (DoS)

Cloud services may be targeted by DoS or DDoS attacks, where attackers flood the infrastructure with excessive traffic, causing service disruptions and making resources unavailable to legitimate users [4-6]. Attackers do not have access to the system and data but turn it into an unusable status.

B. Benefits of Security on the Cloud

Ensuring the security of cloud services is crucial for improving data protection, maintaining reliable service availability, and strengthening corporate reputation and confidence [1-2]. Here are a few benefits of cloud security.

1) Data Protection

Maintaining the confidentiality and integrity of client data and complying with data privacy regulations are essential aspects for cloud service providers and their customers [7-8]. Data can be successfully protected and, as a result, the likelihood of data breaches can be diminished if security is given priority.

2) Service Availability and Reliability

Cloud services are expected to be always available and reliable [9-10]. Implementing robust security measures ensures service continuity and eliminates the impact of potential cyberattacks that can lead to service interruptions and downtime, affecting business operations. By prioritizing security, organizations can reduce the risk of such disruptions.

3) Business Reputation and Trust

The reputation of a cloud service provider can be significantly damaged by a data breach or security incident, resulting in a loss of customer trust [11]. Prioritizing security helps maintain customer confidence and loyalty. For businesses that store proprietary information or intellectual property in the cloud, security is vital to prevent theft or unauthorized access to sensitive data. Furthermore, reputation losses can lead to significant financial losses, both in terms of remediation costs and potential legal liabilities.

4) Emerging Threat Landscape and Resilience to Adversarial Attacks

The cybersecurity threat landscape is constantly evolving. Organizations must focus on security to stay ahead of emerging threats and protect against new attack vectors. Implementing strong security measures in conformity with standards helps cloud-based infrastructures become more resilient to cyber-attacks, making it more challenging for attackers to breach the system.

III. RELATED WORKS FOR INTELLIGENT PREVENTIVE APPROACHES

A. State-of-the-art Cloud Security

Concerning cloud security, many researchers invoke security issues experienced with Software-As-A-Service (SaaS) and Infrastructure-As-A-Service (IaaS) platforms [2-3, 9-11]. The main difficulties related to SaaS mostly involve the management of data stored in cloud applications [7, 11]. The issues include a lack of transparency into data within cloud applications, the risk of data theft by malicious individuals, insufficient control over access to sensitive information, the inability to monitor data while being transferred within cloud applications, a shortage of professionals specializing in cloud security, threats and attacks directed at cloud service providers, and challenges in evaluating the security measures employed by cloud application providers as well as ensuring compliance with regulations. The challenges related to IaaS cover several aspects. These entail the establishment of cloud workloads and accounts that are outside IT visibility, limited control over access to sensitive data, inconsistent security measures in multiple cloud and on-premise environments, sophisticated threats and attacks directed at cloud infrastructure, difficulties in monitoring cloud workload systems and applications for vulnerabilities, and the potential for attacks to spread from one cloud workload to another [15].

In [12], a Machine Learning (ML) technique was developed to identify DDoS threats on cloud computing platforms, implementing the isolation forest anomaly detection technique and correlation to successfully identify DDoS attacks. In [13], a system was proposed to protect against DDoS attacks in the cloud by monitoring performance distortion and detecting multilayer attacks deploying statistical methods. Chi-square statistics were employed to detect differences between regular and attack traffic sources, allowing efficient filtering of attack traffic and protecting cloud infrastructure. In [14], hardware-level attacks, such as Rowhammer and Spectre, were identified in real-time engaging different machine-learning classifiers and tracking variations in microarchitectural events, such as cache misses, to reach a high level of accuracy while maintaining a fair level of performance impact. In [15], security concerns, requirements, and obstacles that cloud service providers encounter in the cloud engineering process were discussed. This study provided recommendations for security standards and management methods to address these concerns, specifically targeting the technical and commercial sectors.

Several studies have proposed resolutions to security concerns utilizing AI. In [16-19], the adoption of intelligent AI strategies was discussed for threat detection, enabling systems to proactively identify risks and respond accordingly. In [20], a comprehensive overview of the capacity of AI to increase cybersecurity was provided in several fields. This review also emphasizes potential subjects for future investigation, involving emerging cybersecurity applications, sophisticated AI methodologies, data representation techniques, and the creation of new infrastructures to enable the smooth integration of AI-based cybersecurity in the current era of digital transformation, which is marked by an intricate network of crises. In [21], a methodical investigation of the existing

literature was carried out to discover studies on cyberattacks that use AI. These studies were analyzed to extract valuable insights for the development of robust cybersecurity solutions. In [22], a concise summary of AI applications in the cybersecurity domain was presented, and methods to enhance protection mechanisms against cyberattacks were investigated. In [23], a comprehensive analysis of the potential benefits and hazards of utilizing AI in cybersecurity was provided. This study also described effective strategies for corporations to reduce these risks.

B. Review of Machine Learning (ML) Algorithms

ML is a prominent aspect of AI that has garnered significant attention due to its crucial role in digitalization solutions [24-26]. This section provides a succinct overview of some commonly employed and widely favored ML methods. The objective is to illuminate the merits and limitations of these algorithms from an application perspective and help readers make well-informed choices when selecting the most appropriate learning algorithm to meet the specific demands of their applications.

1) Logistic Regression (LR)

LR is a statistical method adopted for binary classification that allows the estimation of the likelihood that an observation belongs to one of two possible classes (LR). This algorithm determines the best sigmoid function that transfers input features to probabilities, establishing the association between features and binary output. The sigmoid function's output is bounded inside the range of 0 and 1, which makes it well-suited for describing probabilities. The fundamental stages encompassed in training an LR model include data preprocessing, model training, model prediction, and decision thresholding.

2) Support Vector Machine (SVM)

SVM is a robust supervised ML technique followed for classification and regression tasks [28]. However, its primary reputation lies in its application to binary classification issues. The SVM algorithm operates through a series of four steps: data representation, hyperplane selection, kernel trick, and regularization parameter determination. SVMs are widely recognized for their ability to efficiently manage small- to medium-sized datasets. Training SVMs can be computationally costly when dealing with extremely large datasets. For such situations, it may be preferable to implement approximate algorithms or other techniques such as Stochastic Gradient Descent (SGD). In general, SVM remains a popular and flexible algorithm for classifying and predicting data, especially when dealing with intricate patterns and distinctions.

3) K-Nearest Neighbors (KNN)

KNN is a widely employed and straightforward supervised ML technique deployed for both classification and regression tasks [29]. It is a form of instance-based learning, in which the model uses the proximity of training data points to the new unknown data point it needs to either classify or forecast to generate predictions. The KNN algorithm operates in the following steps: establishing the data representation, determining the optimal value for K, computing the distance metric, making predictions for classification, and finally making prognosis for regression. KNN is commonly utilized as a benchmark method because of its straightforwardness and simplicity of understanding. However, the algorithm's efficiency may decrease when working with data that have a large number of dimensions or datasets with a high number of observations, since the computational load of detecting neighboring data points crucially increases. Although KNN has many drawbacks, it nonetheless bears its significance and is broadly engaged in various ML applications, particularly in situations where there are relatively small datasets and simple decision limits.

4) Naive Bayes (NB)

This approach is called "naive" because it makes a strong assumption that the data attributes are independent of each other for the class label. This former presupposes that each feature makes an independent contribution to the likelihood that a data point is classified into a certain class, which may not always be the case. However, even with this reduction, NB often achieves impressive results in various real-world situations. NB is very valuable for dealing with datasets that have a large number of dimensions, such as text data, where the number of features might be substantial. NB is a fast and computationally inexpensive algorithm that can be efficiently trained on large datasets due to its straightforward design. It has various versions, namely, Gaussian NB, multinomial NB, and Bernoulli NB. Although NB is extensively deployed and easy to apply, its performance may be limited when the condition of independence is violated or when there are high interdependencies across features. However, the NB algorithm remains valuable due to its usefulness as a fast initial model for classification tasks and its effectiveness in dealing with complex data, involving those seen in natural language processing applications.

5) Quadratic Discriminant Analysis (QDA)

QDA is a classification algorithm employed in the fields of ML and statistics. QDA is intricately linked to Linear Discriminant Analysis (LDA), but it permits more adaptable decision boundaries by assuming distinct covariance matrices for each class. QDA necessitates the estimation of a larger number of parameters compared to LDA, particularly when dealing with high-dimensional data, due to the utilization of distinct covariance matrices for each class. This can result in overfitting when training data are scarce. When the number of features greatly exceeds the number of training samples, the estimate of covariance matrices might become unstable. QDA is a valuable classification approach that is applicable when the assumption of distinct covariance matrices is justifiable and the classes have diverse data distributions. It offers a more adaptable method for representing intricate decision boundaries compared to LDA and can be highly competent in many ML tasks, especially when the data lack distinct linear limits.

IV. SECURING CLOUD SERVICES: THE PROPOSED APPROACH

This approach entails a series of interconnected stages, beginning with data collection from network log files. Subsequently, these data are analyzed by a security specialist

who manually annotates them to detect possible patterns of cyberattacks. The IaaS server uses these annotated logs to acquire knowledge and build patterns to anticipate forthcoming attacks and trigger notifications when identifying potential dangers. Consequently, the security administrator evaluates these signals to implement the necessary measures and alleviate any detected hazards. This approach establishes a comprehensive security mechanism to counter cyberattacks in cloud computing settings. Figure 1 presents the proposed framework. The entities being considered are as follows:

- Cloud computing serves as the foundational infrastructure that facilitates the provision and administration of cloud services. It provides scalable and adaptable IT solutions, offering on-demand access to computer resources. The framework can encompass various models, including IaaS, Platform as a Service (PaaS), and SaaS.
- The IaaS server plays a pivotal role as the brain of the operation, hosting advanced software solutions designed to secure these services by analyzing data and identifying potential threats.
- The security expert is a highly skilled individual who meticulously reviews network traffic logs, utilizing his deep understanding of cyber threats to discern between regular activity and potential cyberattacks that could compromise the system's integrity.
- The security administrator is tasked with a critical role, responding promptly to alerts generated by the IaaS and orchestrating the necessary administrative maneuvers to reinforce the security posture of the cloud infrastructure.

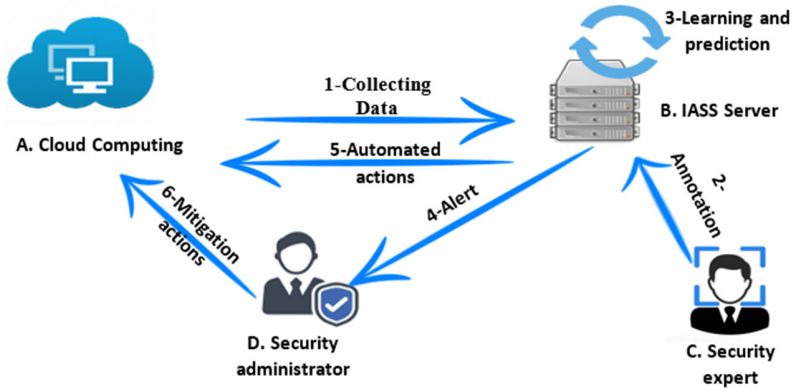


Fig. 1. Proposed architecture for intelligent securing services.

This structured schema articulates the collaboration between human expertise and intelligent systems to ensure robust security in cloud computing environments. Certainly, expanding on the approach would involve detailing the specific methods and technologies followed during each step.

- Data collection: This phase, where network log files are meticulously collected, is foundational. These logs consist of detailed records of network activity, including timestamps, source and destination IP addresses, protocol details, and payload snippets, which could provide evidence of anomalous behavior indicative of cyber threats.
- Annotation: At this stage, a domain expert performs a thorough and manual examination of the logs obtained, exploiting his expertise to identify and categorize patterns that could potentially signify malicious behavior. Annotations act as markers, indicating specific data points that are later used in supervised ML models for training.
- Learning and prediction: The IASS server utilizes the annotated data to train the ML algorithms to identify the designated cyberattack patterns. This training involves the employment of algorithmic models, such as naïve Bayes, KNN, or SVMs, which can acquire knowledge from historical data and make predictions about future events.
- Notification and alert: The IaaS system puts into service advanced predictive algorithms to detect possible security incidents and triggers a sophisticated alerting framework. The purpose of this system is to promptly and effectively notify the security administrator of potential security breaches, guaranteeing a swift response. The prompt notification is essential for reducing the timeframe in which attackers can act, therefore greatly reducing the possible consequences of the cyberattack on the cloud infrastructure.
- Automated responses: The IaaS can initiate countermeasures when it identifies a prospective assault, provided that the attack adheres to specific predetermined criteria and follows some pre-established threat profiles. Upon such recognition, it deploys a series of swift and decisive actions aimed at mitigating the detected threat. These responses, governed by a set of predefined rules, can competently neutralize or significantly diminish the harmful effects of the attack, thereby safeguarding the integrity of the cloud environment. This automated intervention is crucial to maintain continuous operational security, especially in scenarios where human intervention may not be as immediate.
- Mitigation activities: During this phase, the security administrator, upon receiving IaaS notifications, takes

action to implement defensive measures that are specifically designed to address the type and size of the threat. This involves not only updating firewall configurations to prevent unwanted access, but also implementing sophisticated intrusion prevention systems that are specifically designed to anticipate and proactively neutralize attacks. In addition, the administrator has the option to separate specific network parts, thus confining the propagation of the attack and eliminating its operational impact. These activities provide a complex and multilayered defense stance, reinforcing the cloud infrastructure's ability to withstand future cyberattacks.

V. RESULTS AND DISCUSSION

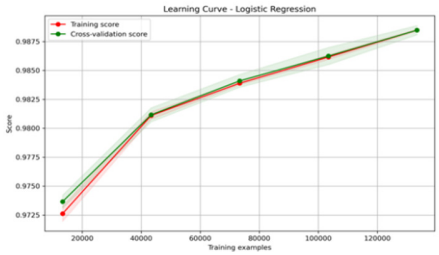
The data employed for evaluating the proposed approach and models were collected from [30]. This dataset encompasses a diverse array of DoS assault categories, rendering it highly helpful for the development and evaluation of DoS detection techniques. The data come in the form of "pcap" files, and they were converted and merged into a single CSV file. The security expert's responsibility includes assessing and classifying each traffic element in the dataset as either a potential DoS attack or not, thus ensuring its up-to-date status. The expert's feedback is integrated into the source file as an additional attribute. Subsequently, the proposed approach employed different predictors and varying dataset sizes: 10,000 (size1), 208,527 (size2), and 1,048,575 (size3) samples. Each data set was partitioned into an 80:20 ratio, with 80% used for training and 20% for testing. The effectiveness of the models was valued by measuring the total accuracy, which is the percentage of predictions that aligned with the actual outcomes. Table I presents the comprehensive accuracy results for each combination of model and dataset size.

TABLE I. ACCURACY OF PREDICTION WITH SELECTED REGRESSORS WITH VARIOUS SAMPLE SIZES

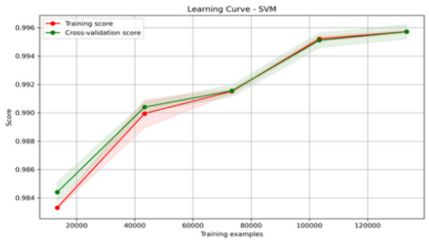
Regressors	Accuracy		
	size 1	size 2	size 3
LR	0.9665	0.990409	0.997502
SVM	0.9855	0.996092	0.998649
KNN	1	0.998945	0.999776
NB	0.6035	0.956002	0.982139
QDA	0.6035	0.587901	0.586791

The SVM, KNN, and LR methods demonstrated satisfactory accuracy, highlighting their efficacy in managing the provided data. There is an interesting pattern displaying that the predicted accuracy of these models noticeably increased with the amount of the dataset. This suggests that the models exhibit scalability and adaptation to additional datasets in addition to maintaining a respectable degree of precision under these settings. The strong results of LR, SVM, and KNN indicate that these models can reliably identify intricate patterns in the data, which adds to their overall competence in predictive modeling situations. It is important to note that this increasing accuracy trajectory with more samples offers insightful information about the scalability and generalization characteristics of the regression approaches used. Figure 2 presents the learning curves of the models.

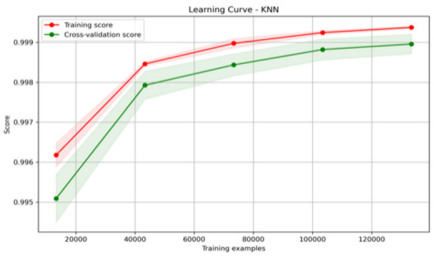
(a)



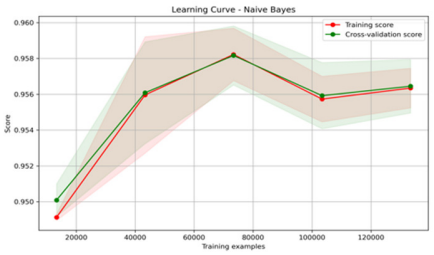
(b)



(c)



(d)



(e)

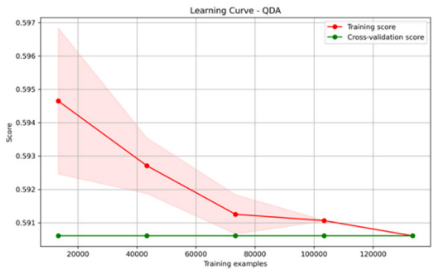


Fig. 2. Learning curves with tested regressors (size 2): (a) LR, (b) SVM, (c) KNN, (d), NB, (e) QDA.

The learning curves provide valuable information on the performance and behavior of the adopted classifiers as the size of the training data rises. The LR curve outlines the method's ability to handle the classification problem. As the size of the training set increases, the regressor shows a significant improvement in accuracy (0.9875), reflecting that it is capable of capturing meaningful patterns. The SVM curve grows with a variable rate and lack of convergence uniformity compared to LR. KNN manifests remarkable behavior on the learning curve, showcasing its strength in capturing localized patterns. Starting

with high accuracy at the initial training sizes, KNN reaches a high score (0.998) with a fast convergence rate. KNN's reliance on local information and its ability to adapt to complex data distributions make it a robust choice, especially when dealing with noisy data. NB reveals an unstable converging rate, as it reaches the highest accuracy of 0.958 and a stabilized accuracy below 0.956. This may be a consequence of assuming independence between features. The QDA learning curve discloses the worst results among the tested regressors and the adopted datasets. This regressor could be effective when the data follows a quadratic decision boundary, but it may not perform optimally in instances with high-dimensional data, which is not the case in this study. Unlike the other regressors, the learning curve of QDA has a negative convergence rate. The learning curves offer valuable insights into the performance of the classification algorithms. KNN stands out in capturing localized patterns with the highest accuracy, SVM demonstrates excellent generalization, and LR shows reliable and consistent performance. NB seems to have unstable convergence, and QDA is not well adapted for this specific classification problem.

The following figures represent the confusion matrices for these regressors according to various sample sizes. Figure 3 illustrates the confusion matrices of the methods with a dataset size of 10,000 (size 1). It should be noted that false positives indicate attacks that have not been recognized yet, whereas false negatives signify cases of missed attack detection. The results from the confusion matrices suggest that KNN is the most accurate regressor overall. KNN constantly performs better than its competitors, exhibiting more predictive power. SVM and LR also provide excellent accuracy, confirming their dependability. A detailed examination signals issues with the QDA and NB, demonstrating a significant rise in false negatives. This points to potential areas for the specific models to be improved and begs the question of how sensitive they are to particular data patterns. In summary, KNN exhibited superior accuracy, SVM and LR functioned well, and NB and QDA deserve further study to improve false negative rates.

Figure 4 presents the confusion matrices for the dataset with a size of 208,527 (size 2). The same perspective and pattern hold as the dataset grows in size. The most reliable regressor is still KNN, which constantly outperforms its competitors. Specifically, false positives are the only incorrect predictions made by LR and QDA. On the other hand, false negatives are more common in QDA for this dataset size. Figure 5 depicts the dataset with a size of 1,048,575 (size 3). KNN continues to produce superior results. KNN recorded 9 false negatives, suggesting that only 9 attack scenarios were missed. The fact that KNN continues to perform better with different dataset sizes highlights its reliability in making accurate predictions regularly. The precise distinction between false positives and false negatives sheds light on the advantages and disadvantages of QDA, LR, and -most importantly- the ongoing dependability of KNN in handling various scenarios.

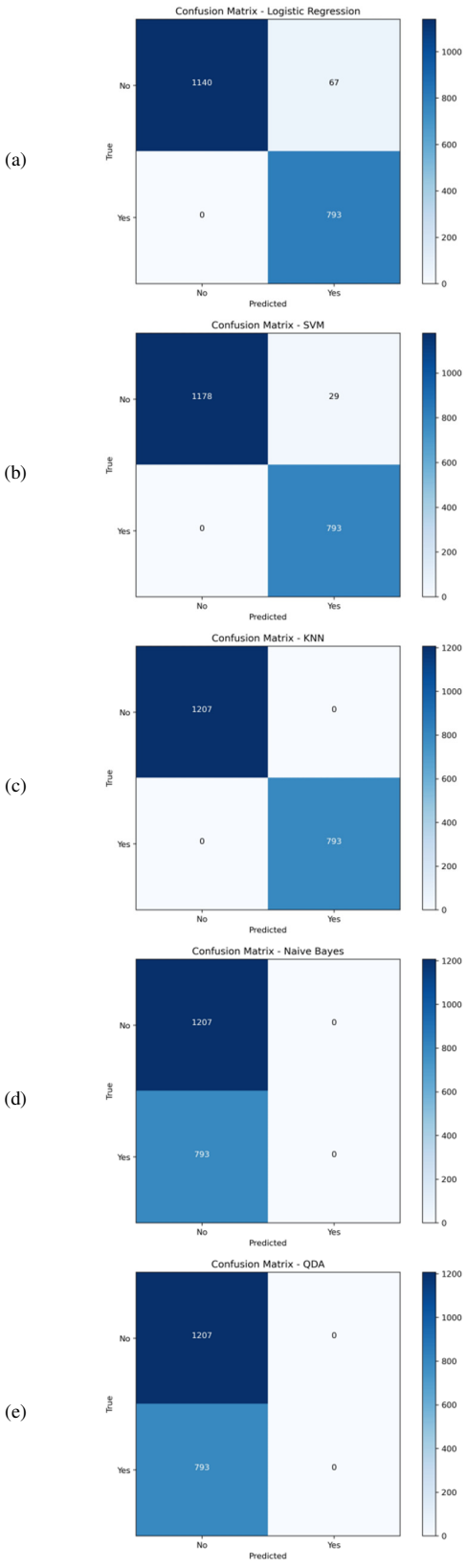


Fig. 3. Confusion matrices for size 1 (10,000): (a) LR, (b) SVM, (c) KNN, (d) NB, (e) QDA.

(a)

(b)

(c)

(d)

(e)

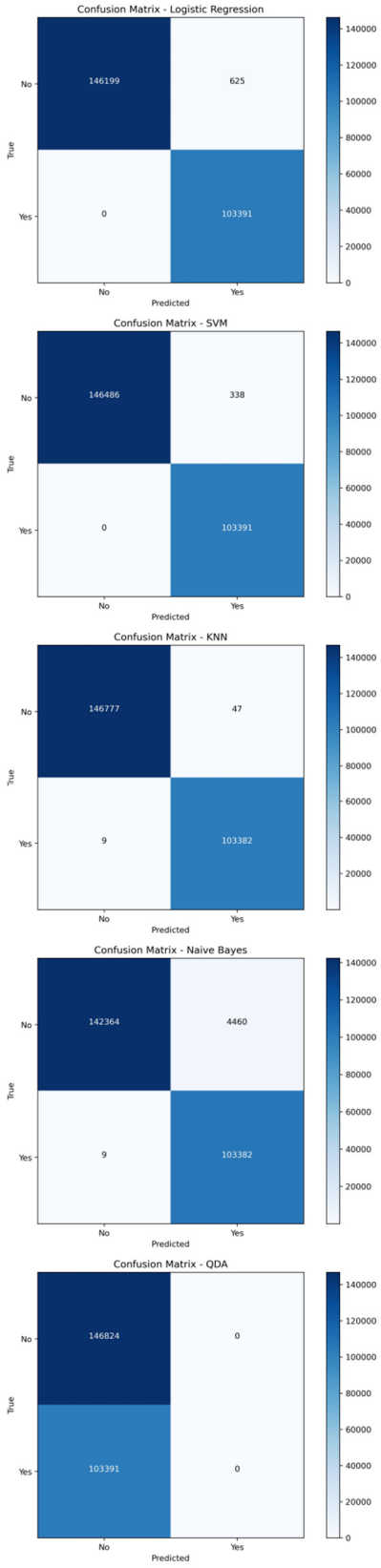


Fig. 4. Confusion matrices for size 3 = 1,048,575: (a) LR, (b) SVM, (c) KNN, (d) NB, (e) QDA.

The KNN was superior to other regressors in minimizing misclassifications, highlighting its flexibility in this particular scenario. Model accuracy can be affected by several factors, and in this case, KNN might be useful since it can recognize localized patterns, which are a common occurrence in DoS attacks. KNN excels in accurate prediction by taking nearby examples of the same class into account. Furthermore, KNN can effectively handle noisy data by reducing the impact of noise and outliers on datasets, such as network traffic log files. However, it is important to recognize that KNN may perform worse in high-dimensional feature spaces, where data points could seem equally distant from a query point, resulting in less accurate recommendations.

VI. CONCLUSION

Research on cloud security mainly emphasizes the technological aspects of security or the involvement of expert human intervention. Conventional methods for preventing DoS attacks often depend on predetermined limits for network traffic. However, this approach can lead to two types of error: false positives, where regular traffic is mistakenly blocked, and false negatives, where malicious traffic is mistakenly allowed. This study used regressors that leverage previous experience to detect DoS attacks. The former contributes to the security of cloud computing by proactively preventing a wide range of attacker scenarios. As a result, the current study guarantees the continuous delivery of cloud services for various demands. A special focus was placed on a sophisticated process that distinguishes ordinary service requests from prospective cybersecurity attacks, where advanced and elaborate countermeasures must be decided. Technology heavily relies on the skillful detection of DoS attacks through cloud traffic. Binary regressors were deployed to systematically analyze previous attack incidences and accurately detect future incidents. If a potential attack is noticed, the system immediately alerts the cloud security administration, allowing swift mobilization and implementation of strategic defenses to minimize any potential damage. The KNN regressor is particularly remarkable in its ability to accurately predict DOS attacks. The results highlight the former's potential to effectively address a broader range of cyber threats. Future endeavors may focus on investigating different attack methods to expand the range of protection provided by the proposed system. Furthermore, the task of handling incomplete datasets, which often arise from heavy traffic or administrative constraints in cloud services, offers a promising area for research. Tackling these obstacles can greatly improve flexibility and the ability to adjust the proposed security system, making it a stronger solution in the ever-changing and fast-moving field of cybersecurity.

ACKNOWLEDGMENT

The authors gratefully acknowledge the approval and support of this study from the Deanship of Scientific Research by the grant CSCR-2022-11-1897, Northern Border University, Arar, Kingdom of Saudi Arabia.

REFERENCES

[1] S. Jones, Z. Irani, U. Sivarajah, and P. E. D. Love, "Risks and rewards of cloud computing in the UK public sector: A reflection on three

Organisational case studies," *Information Systems Frontiers*, vol. 21, no. 2, pp. 359–382, Apr. 2019, https://doi.org/10.1007/s10796-017-9756-0.

[2] A. R. Khan and L. K. Alnwihel, "A Brief Review on Cloud Computing Authentication Frameworks," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 9997–10004, Feb. 2023, https://doi.org/10.48084/etasr.5479.

[3] S. Maroc and J. Zhang, "Comparative Analysis of Cloud Security Classifications, Taxonomies, and Ontologies," in *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science*, Wuhan, China, Apr. 2019, pp. 666–672, https://doi.org/10.1145/3349341.3349487.

[4] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet denial-of-service activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, pp. 115–139, Feb. 2006, https://doi.org/10.1145/1132026.1132027.

[5] M. H. H. Khairi, S. H. S. Ariffin, N. M. A. Latiff, A. S. Abdullah, and M. K. Hassan, "A Review of Anomaly Detection Techniques and Distributed Denial of Service (DDoS) on Software Defined Network (SDN)," *Engineering, Technology & Applied Science Research*, vol. 8, no. 2, pp. 2724–2730, Apr. 2018, https://doi.org/10.48084/etasr.1840.

[6] B. S. K. Devi and T. Subbulakshmi, "Cloud-based DDoS attack detection and defence system using statistical approach," *International Journal of Information and Computer Security*, vol. 11, no. 4–5, pp. 447–475, Jan. 2019, https://doi.org/10.1504/IJICS.2019.101935.

[7] M. Ehsan Ur Rahman and H. D. Sri Saaketh Ram, "AI as a Challenging Problem : Solvable without Data but Morally Intelligence-driven Insights," *International Journal of Scientific Research in Science and Technology*, vol. 6, no. 4, pp. 153–159, Aug. 2019, https://doi.org/10.32628/IJSRST196429.

[8] S. Sharma and S. Khan, "Analysis of Cloud Security, Performance, Scalability and Availability (SPSA)," *International Journal of Scientific Research in Network Security and Communication*, vol. 7, no. 1, pp. 13–15, 2019.

[9] D. Dave, N. Meruliya, T. D. Gajjar, G. T. Ghoda, D. H. Parekh, and R. Sridaran, "Cloud Security Issues and Challenges," in *Big Data Analytics*, Singapore, 2018, pp. 499–514, https://doi.org/10.1007/978-981-10-6620-7_48.

[10] P. Verma, A. Gupta, and R. S. Sambyal, "Security Issues and Challenges in Cloud Computing: A Review," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 4, no. 1, pp. 189–196, 2018.

[11] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 71, pp. 28–42, Oct. 2018, https://doi.org/10.1016/j.compeleceng.2018.06.006.

[12] V. Sharma, V. Verma, and A. Sharma, "Detection of DDoS Attacks Using Machine Learning in Cloud Computing," in *Advanced Informatics for Computing Research*, Shimla, India, 2019, pp. 260–273, https://doi.org/10.1007/978-981-15-0111-1_24.

[13] B. S. K. Devi and T. Subbulakshmi, "Cloud-based DDoS attack detection and defence system using statistical approach," *International Journal of Information and Computer Security*, vol. 11, no. 4–5, pp. 447–475, Jan. 2019, https://doi.org/10.1504/IJICS.2019.101935.

[14] C. Li and J. L. Gaudiot, "Detecting Malicious Attacks Exploiting Hardware Vulnerabilities Using Performance Counters," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Milwaukee, WI, USA, Jul. 2019, vol. 1, pp. 588–597, https://doi.org/10.1109/COMPSAC.2019.00090.

[15] K. Popović and Ž. Hocenski, "Cloud computing security issues and challenges," in *The 33rd International Convention MIPRO*, May 2010, pp. 344–349.

[16] Md. M. Ahmed and A. El-Hajjar, "A Proactive Approach to Protect Cloud Computing Environment Against a Distributed Denial of Service (DDoS) Attack," in *AI, Blockchain and Self-Sovereign Identity in Higher Education*, H. Jahankhani, A. Jamal, G. Brown, E. Sainidis, R. Fong, and U. J. Butt, Eds. Springer Nature Switzerland, 2023, pp. 243–278.

[17] S. Rangaraju, "Ai sentry: Reinventing cybersecurity through intelligent threat detection," *EPH - International Journal of Science And Engineering*, vol. 9, no. 3, pp. 30–35, Dec. 2023, https://doi.org/10.53555/ephijse.v9i3.211.

[18] S. Kuraku, D. Kalla, F. Samaah, and N. Smith, "Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats," *International Journal of Electrical, Electronics and Computers*, vol. 8, no. 6, Nov. 2023.

[19] N. Gupta, R. Agarwal, S. S. Dari, S. Malik, R. Bhatt, and D. Dhabliya, "DDoS and Cyber Attacks Detection and Mitigation in SDN: A Comprehensive Research of Moving Target Defense Systems," in *2023 International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, Jul. 2023, pp. 1–8, https://doi.org/10.1109/ICDSNS58469.2023.10245455.

[20] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, Sep. 2023, Art. no. 101804, https://doi.org/10.1016/j.inffus.2023.101804.

[21] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, vol. 12, no. 8, Jan. 2023, Art. no. 1920, https://doi.org/10.3390/electronics12081920.

[22] E. Yilmaz and O. Can, "Unveiling Shadows: Harnessing Artificial Intelligence for Insider Threat Detection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 2, pp. 13341–13346, Apr. 2024, https://doi.org/10.48084/etasr.6911.

[23] R. Talwar and A. Koury, "Artificial intelligence – the next frontier in IT security?," *Network Security*, vol. 2017, no. 4, pp. 14–17, Apr. 2017, https://doi.org/10.1016/S1353-4858(17)30039-9.

[24] S. Ray, "A Quick Review of Machine Learning Algorithms," in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, Faridabad, India, Feb. 2019, pp. 35–39, https://doi.org/10.1109/COMITCon.2019.8862451.

[25] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, no. 3, Mar. 2021, Art. no. 160, https://doi.org/10.1007/s42979-021-00592-x.

[26] M. Alloghani, D. Al-Jumeily, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science," in *Supervised and Unsupervised Learning for Data Science*, M. W. Berry, A. Mohamed, and B. W. Yap, Eds. Cham: Springer International Publishing, 2020, pp. 3–21.

[27] D. W. H. Jr, S. Lemeshow, and R. X. Sturdivant, *Applied Logistic Regression*. John Wiley & Sons, 2013.

[28] T. B. Trafalis and R. C. Gilbert, "Robust classification and regression using support vector machines," *European Journal of Operational Research*, vol. 173, no. 3, pp. 893–909, Sep. 2006, https://doi.org/10.1016/j.ejor.2005.07.024.

[29] S. Ge, L. Hou U, N. Mamoulis, and D. W. Cheung, "Efficient All Top-k Computation - A Unified Solution for All Top-k, Reverse Top-k and Top-m Influential Queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 5, pp. 1015–1027, Feb. 2013, https://doi.org/10.1109/TKDE.2012.34.

[30] "DDoS evaluation dataset (CIC-DDoS2019)." Canadian Institute for Cybersecurity, [Online]. Available: https://www.unb.ca/cic/datasets/ddos-2019.html.