International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
©2022 INPRESSCO®, All Rights Reserved
Available at http://inpressco.com/category/ijcet

Research Article

Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security

Ramesh Bishukarma*

Lead Engineer, Wing AI Technologies Inc

Received 20 Nov 2022, Accepted 18 Dec 2022, Available online 20 Dec 2022, **Vol.12, No.6 (Nov/Dec 2022)**

Abstract

Cloud computing (CC), particularly through the Software as a Service (SaaS) model, has revolutionized a way organization manage their IT infrastructure. Nonetheless, SaaS has numerous benefits including cost, scalability, and accessibility, and for the same reason, SaaS creates a number of risks. Another important area is anomaly detection on SaaS platforms, so that the identification of abnormal activity may suggest a violation of security, operational deviance, or flawed performance. This paper proposes a novel AI-enabled adaptive anomaly detection method that facilitates the protection of SaaS solutions. Mirroring the ML techniques such as supervised, unsupervised and semi-supervised learning, it provides real-time surveillance of an organization's networks for data breaches, insider threats, malware and denial of service (DoS) attacks. Incorporation of adaptive AI methods enables the framework to learn as well as adapt in the detection of new forms of security threats and hence keep SaaS environments secure. This paper also presents various types of anomalies in SaaS environments, and AI approaches to adaptive SaaS anomaly detection, with focuses on possibilities of these techniques in preserving cloud-based services.

Keywords: *SaaS Security, Cloud Computing, Anomaly Detection, AI-Driven Security, Machine Learning, Deep Learning, Cybersecurity, Adaptive Detection.*

1. Introduction

Cloud computing (CC) provides a shared resource for adaptable computing resources and computing outsourcing procedures, allowing for the provision of a wide range of computing services to both individuals and businesses [1]. Automatic software upgrades, better collaboration, scalability, flexibility, cost effectiveness, and business continuity are just a few of the potential advantages of CC, which has led millions of organisations to embrace it. Numerous services and implementation approaches are included in CC[2][3].

The three service models offered by CC are software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS). IaaS offers choices like virtual or real IT storage and networking capabilities for rent[4], while PaaS offers tools for administration, training, product creation, and delivery on demand. Furthermore, SaaS is a model for delivering cloud-based software applications on demand via subscription [5][6].

SaaS refers to a software deployment paradigm in which clients have access to applications over the Internet on demand from service providers or applications hosted elsewhere [7][8][9]. Customers gain from the SaaS model in a number of ways, including lower costs and more operational efficiency. SaaS is quickly becoming the go-to approach for meeting the demands of corporate IT services[10][11]. Instead than downloading and installing software on individual computers, users may access their apps via a web browser using SaaS [4][12]. It is a method for managing security in a cloud computing setting via outsourcing [13][14][15].

One of the most crucial ideas in data analysis is anomaly detection. If an information item deviates substantially from typical data behaviour in certain areas, it is deemed an anomaly. Generally speaking, it indicates that the item in a given data array is unique[16].

Anomalies in a cloud network signify deviations from expected patterns, behaviours, and occurrences, potentially indicating security threats, operational irregularities, or performance issues. Categorized into types such as security[17], network traffic, resource utilization, application behaviour, data, and user behaviour anomalies, they encompass unauthorized access, unusual data transmission, and abnormal resource use[18][19]. Recognizing and addressing these anomalies is crucial for preserving the cloud network's integrity, security, and reliability, safeguarding against cyber threats, and ensuring optimal performance[20].

*Corresponding author's ORCID ID: 0000-0000-0000-0000

DOI: https://doi.org/10.14741/ijcet/v.12.6.8

Anomaly detection over encrypted communications is a practical use of AI technology such as DL and ML [21][22]. Thus, there is a strong emphasis on AI-based anomaly detection over encrypted communication. analysed encrypted communications for anomaly detection using XGBoost and SVM, two conventional ML techniques. study using CNN and LSTM, two DL algorithms, to identify anomalies in encrypted communications[23]. Research on AI anomaly detection over encrypted communications is ongoing, but there hasn't been nearly enough systematic examination of the literature on the topic[24].

Organization of the paper

This paper is organised in the following way: Section II looks at a current state of SaaS security threats. In Section III, a brief on anomaly detection in cybersecurity is provided. Section IV discuss the Ai-driven techniques for adaptive anomaly detection. Ans Then section V provide the Anomaly Detection Framework for SaaS Platform. Section VI provide Related Work and last section VII discussed conclusion and future work.

2. Current state of Saas security threats

This is the first layer of the service model. In this cloud model, providers offer database and software access, but Software as-a-service (SaaS) faces security challenges, putting responsibility on users. Users must be cautious about shared information and access. Recent cyber threats highlight the appeal of cloud providers as targets, requiring users to scrutinize provider security [25].

Business Services
Document Management
1
2
SaaS
3
4
Social Networks
Mail Services

Figure 1: SaaS in cloud computing

SaaS is a popular CC service model, but unlike other CC models, it relies heavily on third parties, which makes security a big concern (see Figure 1). SaaS security measures are those that protect company data and user privacy in cloud apps that are accessible via subscription. Many users, using almost any device, have access to the mountain of personal data stored by SaaS services, which poses a threat to both privacy and the security of vital information[26]. Until recently, many businesses' main applications and data were stored on internal servers. When it comes to security, this puts the whole weight of proof on the operator. However, at least it's clear what has to be covered and how. Security issues, however, became increasingly prevalent as more businesses used SaaS solutions. Cloud hosting poses additional security risks for SaaS applications, including the possibility of data breaches and the introduction of malicious software or phishing attempts [27][11].

Types of SaaS threat

Description of internal and external threats, such as unauthorized access, DDoS attacks, and malware.

A. Internal Attacks: The opposite is true with internal dangers; we are used to them. They don't generally go outside the "perimeter" and are what most people image when they think of cyber risks in general. Is employed by the cloud service provider, client or other third-party provider organisation supporting the operation of a cloud service. Cloud services, client data, and supporting infrastructure and apps may be accessible to them, depending on their position in the organisation [28].
B. External Attacks: External threats are those that come from sources outside the network, such as the general public and international news. Does not work for the company providing the cloud service, the client, or any other third party that helps run the cloud service. Is not authorised to access customer data, cloud services, or any of the applications or infrastructure that support them. Attacks cloud service providers, customers, or third-party supporting organisations by taking advantage of security flaws in their systems, procedures, and people in order to compromise the privacy, security, and availability of their data [28].
C. DDOS Attack: Security breaches result in DoS attacks. It blocks certain cloud systems, devices, or resources from being accessed by authorised customers. DDoS assaults are carried out via a network of zombies, which are nodes that are remotely controlled, well-structured, and dispersed. The assailant launches the assault with the assistance of secondary victims, who are zombies [29].
D. Malware Attack: Software with the intent to damage a system or steal data is known as malware. It spreads via a number of executable or software vectors and engages in illegal acts such as data breaches and identity theft [30].

SaaS Security Risks and Challenges

Cloud-based applications and services have transformed businesses with software as a service (SaaS). There are several security concerns with SaaS, despite its many advantages. Here are a few of the most common threats to SaaS security:

A. Lack of control: Cloud-based SaaS providers typically host data and applications, making SaaS application security less controllable for consumers. As a result, customers may find it difficult to monitor and manage their security effectively.

B. Data breaches: Many sensitive data sets are stored in the cloud with SaaS solutions. Without proper security measures, this data can be vulnerable to breaches. A SaaS provider’s infrastructure or user accounts may be exploited by attackers, resulting in data compromise.

C. Insider threats: Customers' data is accessible to SaaS providers, and insider threats might be posed by staff of these companies. Despite stringent security measures implemented by reputable providers, the possibility of insider mishandling or accessing sensitive data remains a concern.

D. Regulatory compliance: There are different privacy and data protection laws in different industries and regions. SaaS providers must comply with these regulations before organizations adopt them. Keeping data secure, transferring data cross-border, and complying with third-party services can be quite challenging.

E. Data loss and availability: Cloud infrastructure is critical to the availability and reliability of SaaS applications. When vital apps and data become inaccessible due to system outages or interruptions, it may have a negative impact on business operations. Data loss may occur in a SaaS environment due to inadvertent deletion or corruption if backup and recovery procedures are not established.

F. Integration vulnerabilities: Integrating SaaS apps with other systems and services is common practice in an organization's ecosystem. Integrations that are not secure can be used by attackers as entry points. For access to data and leaks of information, integrators must be assessed and monitored carefully [31].

3. Anomaly detection in cybersecurity

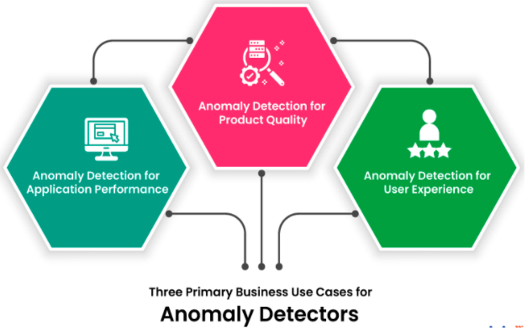
Anomaly Detection for Product Quality
Anomaly Detection for Application Performance
Anomaly Detection for User Experience
Three Primary Business Use Cases for
Anomaly Detectors

Figure 2: Anomaly detection

To understand the evolution of anomaly detection in cybersecurity, it is essential to trace its foundations. Traditional systems that relied on signatures were good at detecting known threats but had a hard time seeing more complex or new assaults. With the introduction of ML, a new era began, one in which systems could learn from data patterns and adjust to new dangers [32]. Figure 2 shows how the ADS works as an intrusion detection system approach to find out-of-the-ordinary system activity.

Types of Anomalies in SaaS Environments

A. Behavioral Anomalies: Your network security depends on behaviour anomaly detection tools since they enable your IT staff to identify any odd activity. The need of using Behaviour Anomaly Detection technologies to ensure the safety of your company was covered in this article. Maintaining the security of your network is a complex process that requires many stages.

B. Operational Anomalies: Operations Anomalies identifies unusual or unexpected API data patterns on your APIs, based on recent data patterns. Operations abnormalities keeps a close eye on API data and uses statistical analysis to separate real abnormalities from chance variations. Operations Anomalies shows the anomaly information on the Operations Anomalies dashboard when it finds one.

C. Data Anomalies: Data anomalies are instances when the observed patterns or norms do not match up with the predicted ones in a dataset. Issues concerning data processing, analysis, and especially, interpretation might ensue when all those outsiders reveal themselves as flaws in the data set. In a DBMS, data anomalies can render the data useless or of very little value, meaning that the usage of the data is significantly reduced.

4. AI-driven techniques for adaptive anomaly detection

Anomaly detection methods that use labelled training are defined as supervised. To train their algorithms, supervised methods need training data, which may be costly to acquire, and these methods struggle to identify novel forms of attack. Semi-supervised approaches utilise just a minimal quantity of labelled data to create a model that detects abnormalities. Unsupervised approaches don't need any training data and may identify previously unknown assaults [33].

Understanding Machine Learning Algorithms techniques

The term "machine learning" refers to a wide variety of algorithms, each of which is designed to meet particular requirements within the field of cybersecurity. This subsection offers a summary of the fundamental ideas, which are as follows:

A. Supervised Learning: Interestingly, the supervised learning system makes models learn with the help of datasets which have been labelled sort of the input data is tied down to the output labels that are implicit on it. In order to complete tasks such as classification and regression, this approach is absolutely necessary[34]. Additionally, there are two main types of supervised anomaly detection methods: signature-based and anomaly-based. The former requires a deep understanding of what makes cyberattacks unique; more specifically, the attack's signature is the main indicator of suspicious activity[35]
B. Unsupervised Learning: Discovering hidden patterns or groups is the goal of unsupervised learning, which involves training models on data that has not been labelled. In cybersecurity, two of the applications that are commonly implemented are clustering and dimensionality reduction [36].
C. Semi-Supervised Learning: The main application of semi-supervised learning to combine aspects of both supervised and unsupervised learning turns out to be advantageous when the amount of labelled data is limited while the amount of unlabelled data is abundant and vice versa. the proposed semi-supervised methods fall under the umbrella of supervised methods of anomaly detection which enable the training of models using vast amounts of unlabelled data and limited labelled data [37].

Advantages of machine learning for anomaly detection

Differently from traditional models, ML models have limited need for communication and can learn and operate continually. We move to look at some of the benefits that are often associated with each of them in this area [38].

A. Adaptability: New data, in that case, helps the ML models to keep on learning and be improved over a particular period. This helps them to spot hitherto unseen patterns of irregularity and defend against new forms of assault. An ML model that has recently been trained on network traffic data may for instance adapt to be able to recognize new strains of malware that communicate differently from other strains of malware.
B. Pattern recognition: Intuitively, it is worth noting that using ML algorithms allow us to identify very fine hierarchies within a given data set. This makes it possible for them to notice anomalies that conventional rule-based systems might fail to notice. An ML model evaluating user log in data for example may come across such oddities as login conducted at odd hour or from odd location suggesting a hacked account.
C. Reduced false positives: The amount of false positives produced by conventional IDS may be decreased by using ML models that can distinguish between normal and abnormal behaviour with the right training and tuning. By concentrating on real risks, this lessens the workload for security analysts. Additionally, it removes the possibility that accurate data would be mistaken for flawed data. This is among the typical drawbacks of conventional models.
D. Scalability: Due to efficiency in processing large and complex data, ML models are suitable for protecting large networks such as extensive systems. This is to support organizations that transact with large volumes of data generated by distributed computing systems, cloud environments and IoT gadgets.

5. Anomaly detection system for saas platform security

Smart anomaly detection is critical in defending SaaS from different type security risks including intrusion, fraudulence, and system weaknesses[39]. An example of using anomaly detection system is to solve the problem of detecting potential threats before they become serious security threats. For instance, if a person who often logs in from one place suddenly logs in from another completely different region, then there is high possibility of account breach.

Data Collection and Normalization: SaaS platforms therefore need to gather information from other sources such as logs of user activities, traffic in the network, calls to APIs, and overall behaviours of the whole system to check for anomalies. This data needs to be normalized to bring it to a format that is easily recognizable so as to be measured against a norm. For instance, if a user has frequently used some features in a particular platform, this activity will feature in the data as the initial point of reference for further comparison[40].

Establishing Behavioral Baselines: The baseline behavior after gathering the data is identifying normal activities or states for the analyzed subjects. These baselines are basic usage characteristics expected of a user or system, for example the frequency of login attempts, usage frequencies or data access frequency of a user. For instance, if a user logs in every day with time at 9 AM, then it becomes one's default behavior. Any variation such as multiple login attempt at midnight from different IP address would then raise an alarm for security threats[41].

Anomaly Detection Algorithms: There are numerous ways by which the anomaly can be detected, depending on the applied algorithms. To know what exactly is considered 'very atypical' or 'very unlikely', statisticians then use the z-scores. Other types of the ML capable of analyzing complex data are clustering and DL tools such as autoencoders. For example, an unsupervised learning model could point out an increasing rate of usage of API from a specific IP address, which may suggest that the platform is under the DDoS attack[42].

Types of Anomalies to Detect: SaaS platforms need to detect different types of anomalies based on their security requirements. For instance, it is easy to identify attempts by unauthorized persons to log into a system through recognizing logins from new places, or detecting high levels of data accesses or sensitive data. For instance, if a user usually works only with their files but today downloaded a lot of files with restricted access, such action would be qualified as suspicious[43].

Real-time Monitoring and Alerts: Anomaly detection can easily be accomplished but real-time monitoring and the ability to trigger an alert that can be responded to is vital. When an anomaly is detected, the system should alert security teams or take or initiate a certain action, it should lock the account for sometime or get multi-factor authentication. For instance, if the IP address of the user changes frequently in a relatively short time, then the operation system can lock the account and make the security team know to take further action[44].

Visualization and Reporting: Security teams use visualization tools to watch the machines and understand what the existing variations are. Dashboards offer real-time view of threats, current trends and past trends that a team or organization can look at in order to find a pattern or a chink in the wall. For instance, a graph with the number of unsuccessful logins through a given period could mean a Brute Force attack on the platform in need of a closer inspection/reaction.

Challenges in Anomaly Detection: A major issue with anomaly detection is that is often tends to produce a lot of false positives when there is is a large number of false alarms. For instance, if a user is traveling for business and logs in from a different country, the system will likely report this as suspicious though it is not. In the same way, since the nature of threats evolves over time, anomaly detection also has to be adapted to constantly update the sensors needed to monitor threats.

Integration with Other Security Measures: Anomaly detection can be therefore combined with other components as IDS or with other threat intelligence feeds to increase platform security. For example, an anomaly detection system could work in tandem with threat intelligence to identify known attack patterns, helping to filter out false positives and improve detection accuracy. An automated response mechanism, like blocking suspicious IP addresses or requiring additional authentication steps, can further mitigate the risk.

6. Literature review

The following previous research on Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security.

In this research, (Yen et al., 2017), advocated for a paradigm for manufacturing system health monitoring that is focused upon SaaS. Thanks to SaaS's adaptability and simplicity, data, processes, and technology may be easily shared and reused. Important technologies for the framework are also investigated, in addition to the overall framework. They list the gaps after reviewing the literature on time series data storage and methods for mining associated data. As a means of communication, they go over possible solutions to the issues. Plus, they think about how to integrate the possible methods into their system for efficient defect identification and diagnosis[45], .

In this, (Kohyarnejadfard et al., 2021), study provided a framework for detecting anomalies in trace data, which not only helps engineers find performance issues but also shortens the time spent debugging. Employing the Linux Trace Toolkit Next Generation, their framework gathers system call streams while processes run. A ML module then uses the streams to identify subsequences of calls that are unusual in terms of frequency and timing of execution. Their technique successfully differentiates between normal and aberrant sequences in extensive trials conducted on actual datasets from two apps (e.g., MySQL and Chrome) under diverse situations using the available labelled data[46], .

In this, (Zhang et al., 2018), studyexamines the critical components of a SaaS platform for industrial chain coordination, including the security, encryption, and configuration needs of multi-tenant business data. Lastly, the platform data is used for user authentication, hierarchical decryption queries, key configuration management, authorisation configuration management, and verification. The findings demonstrate that various coalitions may achieve their personalised data encryption needs via corporate champion configuration[47], .

In this, (Ghafari and Safavi Hemami, 2021), study proposed a method for securing cloud gaming servers with SDN-based anomaly detection; to accomplish their test penetration, they employed SDN to build game streaming. Their SDN-based database was also constructed using an aggressive methodology. In this task, three malicious actors find numerous entry points into the cloud gaming infrastructure in order to obstruct the player's and server's access during concurrent game streaming. They built a NN to evaluate and identify anomalies using the event data stored in the controller. Their controller can identify abnormalities effectively and with minimal mistake, according to numerical data[48], .

In this,(Son et al., 2021), study differentiate abnormalities as erroneous data from those pertaining to the condition of structures or sensor equipment, and provide a system to detect both types of anomalies. They learn temporal correlation and handle multivariate time series using an encoder-decoder architecture based on a LSTM network. An anomaly is found when the trained LSTM network calculates an anomaly score. Using cable tension data collected from a real cable-stayed bridge, they assess the suggested method[49].

In this study,(Frattini et al., 2014), examine the thoroughness and accuracy of an invariant-based anomaly detection system. They have chosen to examine a SaaS platform's back-end functioning as our case study. Results demonstrate the logic of the technique and illustrate how the invariant mining strategy affects detection accuracy and time to disclose violations. When everything goes according to plan, a system is said to have invariants, which are its predicted qualities. An anomaly in the system is most usually associated with the violation of an invariant[50], .

Table 1 organizes the contributions of each research, summarizing the key findings on the Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security.

Table 1: Summary of literature Review on Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security

Study	Focus Area	Key Methodologies	Key Findings	Limitations	Future Work
[45]	SaaS-centered framework for manufacturing system health management	Framework design, time series data storage, mining correlated data	Framework facilitates reuse and sharing of data/processes; identified methods for fault detection and diagnosis	Limited to manufacturing systems; lacks focus on real-time anomaly detection for security	Explore real-time anomaly detection techniques; apply framework to broader SaaS applications
[46]	Anomaly detection for performance troubleshooting	Linux Trace Toolkit Next Generation, Machine Learning on system calls	Effective in reducing troubleshooting time and identifying performance issues in trace data	Limited to system call anomalies; dependency on labeled data	Extend to other types of anomaly data; improve model for scenarios with sparse labels
[47]	Multi-tenant data encryption for industrial SaaS	Encryption configuration algorithm, data-driven encryption, decryption query	Achieves personalized data encryption for multi-tenant environments; enhances authorization and identity management	Focuses primarily on data encryption, not comprehensive anomaly detection	Integrate with anomaly detection for encrypted environments; expand to other security layers
[48]	Anomaly detection in cloud gaming with SDN	Software Defined Network (SDN), Neural Network (NN)	SDN-based NN effectively detects anomalies with low error during game streaming attacks	Limited to cloud gaming; lacks adaptability to different SaaS platforms	Generalize model to various SaaS scenarios; incorporate adaptive learning to handle evolving threats
[49]	Differentiating data inaccuracies from structural anomalies	LSTM Encoder-Decoder, multivariate time series, anomaly scoring	Effectively distinguishes between sensor/data inaccuracies and structural anomalies	Application-specific (bridge monitoring); high computational cost of LSTM models	Apply framework to general SaaS anomaly detection; explore lighter models for real-time use
[50]	Anomaly detection via system invariants in SaaS back-end operations	Invariant mining, anomaly scoring	Invariant mining provides accurate detection with minimal false positives; useful for SaaS operational monitoring	Limited to back-end anomalies; invariant mining may not capture dynamic anomalies	Explore dynamic invariants for broader anomaly coverage; adapt method for front-end SaaS components

Conclusion and future work

The evolvement of SaaS platforms have dramatically affected processes corporate management and growth, yet it introduces serious security concerns. The proposed adaptive AI-based anomaly detection framework covered in this paper aligns well to address these security concerns. This way, the framework guarantees that SaaS platforms can detect the known and unknown deviations using the machine learning techniques required to prevent a vast number of cyber threats, including unauthorized access, malware attacks, and data breaches. Through its training, the AI models designed also have the capacity to learn from new data in order to improve the models' ability to detect emerging threats. As a result of enhanced anomaly detection performance which this framework minimizes false positives, security teams can easily focus on real threats. Given the dynamic nature of threat landscape in cyberspace, effective and efficient intelligent, scalable and adaptive security solutions become a necessity. The work in future ought to consider high level deep learning methods and real time data processing with a view of enhancing SaaS security and guarantee the continual protection of first-class user information in cloud environment.

As for future work, in-app development of real-time AI models that are selective for lightweight cloud environments should be the focus to enable scalability for accomplishing large-scale anomaly detection. Other methods such as FL and HE are also relevant to protect the user data in the shared cloud environment without necessarily compromising on the security of the users. Further to this, increasing the deployment of unsupervised and semi-supervised learning models to improve detection can also improve the ability to detect threats not previously encountered in data-poor contexts. Moreover, integrating multi-source data from application logs, user behavior analytics, and network traffic into a unified detection framework can lead to a more holistic and robust approach. The next steps should include enhancing explain ability in AI models to improve trust and usability, especially for security teams, and embedding adaptive anomaly detection frameworks into zero-trust security models to create a more resilient and scalable defense for SaaS applications. These advancements will be pivotal as SaaS adoption grows, providing a robust security foundation for future cloud-based applications.

References

[1] S. G. Ankur Kushwaha, Priya Pathak, "Review of optimize load balancing algorithms in cloud," *Int. J. Distrib. Cloud Comput.*, vol. 4, no. 2, pp. 1–9, 2016.

[2] R. Arora, S. Gera, and M. Saxena, "Mitigating Security Risks on Privacy of Sensitive Data used in Cloud-based ERP Applications," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 458–463.

[3] M. S. Rajeev Arora, "Applications of Cloud Based ERP Application and how to address Security and Data Privacy Issues in Cloud application," *Himal. Univ.*, 2022.

[4] M. S. Rajeev Arora, Sheetal Gera, "Impact of Cloud Computing Services and Application in Healthcare Sector and to provide improved quality patient care," *IEEE Int. Conf. Cloud Comput. Emerg. Mark. (CCEM), NJ, USA, 2021*, pp. 45–47, 2021.

[5] M. Alshehri, "An Effective Mechanism for Selection of a Cloud Service Provider Using Cosine Maximization Method," *Arab. J. Sci. Eng.*, 2019, doi: 10.1007/s13369-019-03947-y.

[6] R. Goyal, "The Role Of Business Analysts In Information Management Projects," *Int. J. Core Eng. Manag.*, vol. 6, no. 9, pp. 76–86, 2020.

[7] K. K. SKR Anumandla, VK Yarlagadda, SCR Vennapusa, "Unveiling the Influence of Artificial Intelligence on Resource Management and Sustainable Development: A Comprehensive Investigation," *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2020.

[8] V. K. Y. Mohamed Ali Shajahan, Nicholas Richardson, Niravkumar Dhameliya, Bhavik Patel, Sunil Kumar Reddy Anumandla, "AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development," *Eng. Int.*, vol. 7, no. 2, pp. 161–178, 2019.

[9] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of elevator controllers for energy efficiency," in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2012. doi: 10.1109/ISCE.2012.6241747.

[10] V. K. Yarlagadda and R. Pydipalli, "Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity," *Eng. Int.*, vol. 6, no. 2, pp. 211–222, Dec. 2018, doi: 10.18034/ei.v6i2.709.

[11] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, "Role-Based Access Control in SAS Programming: Enhancing Security and Authorization," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[12] A. P. A. Singh and N. Gameti, "Streamlining Purchase Requisitions and Orders : A Guide to Effective Goods Receipt Management," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 5, pp. g179–g184, 2021.

[13] V. A and T. Singh Randhawa, "A Case Study : Security as A Service (SAAS) in Cloud Computing Environment," *Int. J. Sci. Res. Sci. Technol.*, vol. 4, no. 11, pp. 105–111, 2018, doi: 10.32628/ijsrst18401110.

[14] V. V. Kumar and F. T. S. Chan, "A superiority search and optimisation algorithm to solve RFID and an environmental factor embedded closed loop logistics model," *Int. J. Prod. Res.*, 2011, doi: 10.1080/00207543.2010.503201.

[15] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, "Assessment and improvement of intelligent controllers for elevator energy efficiency," in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.

[16] A. G. Shoro and T. R. Soomro, "Big Data Analysis: Ap Spark Perspective," 2015.

[17] J. Thomas, "Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning: A Case Study of Logistics," *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 9, 2021.

[18] J. Thomas, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[19] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, "Performance evaluation of energy efficient intelligent elevator controllers," in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

[20] Y. Liu, Z. Pang, M. Karlsson, and S. Gong, "Anomaly detection based on machine learning in IoT-based vertical plant wall for indoor climate control," *Build. Environ.*, 2020, doi: 10.1016/j.buildenv.2020.107212.

[21] K. Cho *et al.*, "Learning phrase representations using RNN encoder-decoder for statistical machine translation," in *EMNLP 2014 - 2014 Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference*, 2014. doi: 10.3115/v1/d14-1179.

[22] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, "Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making," *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.

[23] L. Chen, S. Gao, B. Liu, Z. Lu, and Z. Jiang, "THS-IDPC: A three-stage hierarchical sampling method based on improved density peaks clustering algorithm for encrypted malicious traffic detection," *J. Supercomput.*, 2020, doi: 10.1007/s11227-020-03372-1.

[24] D. Moher *et al.*, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," 2009. doi: 10.1371/journal.pmed.1000097.

[25] A. Shajan and S. Rangaswamy, "Survey of Security Threats and Countermeasures in Cloud Computing," *United Int. J. Res. Technol.*, 2021.

[26] P. Chouhan, F. Yao, S. Y, and S. Sezer, "Software as a Service: Analyzing Security Issues," *Cent. Secur. Inf. Technol.*, 2014.

[27] A. A. Soofi, M. I. Khan, R. Talib, and U. Sarwar, "Security Issues in SaaS Delivery Model of Cloud Computing," vol. 3, no. 3, pp. 15–21, 2014.

[28] T. TagElsir Ahmed Osman, A. A. babiker, and N. Mustafa, "Internal & External Attacks in cloud computing Environment from confidentiality, integrity and availability points of view," *IOSR J. Comput. Eng. Ver. V*, 2015.

[29] S. A. Varma and K. G. Reddy, "A Review of DDoS Attacks and its Countermeasures in Cloud Computing," in *2021 5th International Conference on Information Systems and Computer Networks, ISCON 2021*, 2021. doi: 10.1109/ISCON52037.2021.9702388.

[30] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," *ACM Comput. Surv.*, 2017, doi: 10.1145/3073559.

[31] P. K. Chouhan, F. Yao, and S. Sezer, "Software as a service: Understanding security issues," in *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 2015. doi: 10.1109/SAI.2015.7237140.

[32] T. Barbariol, E. Feltresi, and G. A. Susto, "Machine Learning approaches for Anomaly Detection in Multiphase Flow Meters," *IFAC-PapersOnLine*, vol. 52, no. 11, pp. 212–217, 2019, doi: 10.1016/j.ifacol.2019.09.143.

[33] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," 2016. doi: 10.1016/j.jnca.2015.11.016.

[34] S. B. and S. C. and S. Clarita, "AN ANALYSIS: EARLY DIAGNOSIS AND CLASSIFICATION OF PARKINSON'S DISEASE USING MACHINE LEARNING TECHNIQUES," *Int. J. Comput. Eng. Technol.*, vol. 12, no. 01, pp. 54-66., 2021, doi: http://www.iaeme.com/IJCET/issues.asp?JType=IJCET&VType=12&IType=1.

[35] C. W. Ten, J. Hong, and C. C. Liu, "Anomaly detection for cybersecurity of the substations," *IEEE Trans. Smart Grid*, 2011, doi: 10.1109/TSG.2011.2159406.

[36] D. A. Bierbrauer, A. Chang, W. Kritzer, and N. D. Bastian, "Anomaly Detection in Cybersecurity: Unsupervised, Graph-Based and Supervised Learning Methods in Adversarial Environments," *Cryptogr. Secur. (cs.CR); Artif. Intell. (cs.AI); Mach. Learn.*, 2021.

[37] J. E. van Engelen and H. H. Hoos, "A survey on semi-supervised learning," *Mach. Learn.*, 2020, doi: 10.1007/s10994-019-05855-6.

[38] S. Wang, J. F. Balarezo, S. Kandeepan, A. Al-Hourani, K. G. Chavez, and B. Rubinstein, "Machine learning in network anomaly detection: A survey," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3126834.

[39] R. Bishukarma, "The Role of AI in Automated Testing and Monitoring in SaaS Environments," *Int. J. Res. Anal. Rev.*, vol. 8, no. 2, pp. 846–852, 2021, [Online]. Available: https://www.ijrar.org/papers/IJRAR21B2597.pdf

[40] I. F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Comput. Networks*, 2021, doi: 10.1016/j.comnet.2021.107840.

[41] A. M. Fawaz and W. H. Sanders, "Learning process behavioral baselines for anomaly detection," in *Proceedings of IEEE Pacific Rim International Symposium on Dependable Computing, PRDC*, 2017. doi: 10.1109/PRDC.2017.28.

[42] J. Kim, M. Park, H. Kim, S. Cho, and P. Kang, "Insider threat detection based on user behavior modeling and anomaly detection algorithms," *Appl. Sci.*, 2019, doi: 10.3390/app9194018.

[43] S. Ranshous, S. Shen, D. Koutra, S. Harenberg, C. Faloutsos, and N. F. Samatova, "Anomaly detection in dynamic networks: A survey," 2015. doi: 10.1002/wics.1347.

[44] J. Musinsky *et al.*, "Conservation impacts of a near real-time forest monitoring and alert system for the tropics," *Remote Sens. Ecol. Conserv.*, 2018, doi: 10.1002/rse2.78.

[45] I.-L. Yen, S. Zhang, F. Bastani, and Y. Zhang, "A Framework for IoT-Based Monitoring and Diagnosis of Manufacturing Systems," in *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2017, pp. 1–8. doi: 10.1109/SOSE.2017.26.

[46] I. Kohyarnejadfard, D. Aloise, M. R. Dagenais, and M. Shakeri, "A Framework for Detecting System Performance Anomalies Using Tracing Data Analysis," *Entropy*, vol. 23, no. 8, 2021, doi: 10.3390/e23081011.

[47] Y. Zhang, H. Sheng, X. Wang, and J. Hua, "User security authentication scheme under saas platform of enterprises," in *Proceedings - 2018 International Conference on Virtual Reality and Intelligent Systems, ICVRIS 2018*, 2018. doi: 10.1109/ICVRIS.2018.00043.

[48] M. Ghafari and S. M. Safavi Hemami, "SDN-based Deep Anomaly Detection for Securing Cloud Gaming Servers," in *2021 12th International Conference on Information and Knowledge Technology (IKT)*, 2021, pp. 67–71. doi: 10.1109/IKT54664.2021.9685665.

[49] H. Son, Y. Jang, S. E. Kim, D. Kim, and J. W. Park, "Deep Learning-Based Anomaly Detection to Classify Inaccurate Data and Damaged Condition of a Cable-Stayed Bridge," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3100419.

[50] F. Frattini, S. Sarkar, J. N. Khasnabish, and S. Russo, "Using invariants for anomaly detection: The case study of a SaaS application," in *Proceedings - IEEE 25th International Symposium on Software Reliability Engineering Workshops, ISSREW 2014*, 2014. doi: 10.1109/ISSREW.2014.57.