aajed.com ISSN 3067-4190

AMERICAN ADVANCED JOURNAL FOR EMERGING DISCIPLINARIES (AAJED)

OPEN ACCESS. PEER-REVIEWED. GLOBALLY FOCUSED.

Artificial Intelligence and Infrastructure-as-Code: Revolutionizing Cloud Computing Security for Retail Operations

Chandrashekar Pandugula,
Sr Data Engineer, Lowes Inc
NC, USA

Abstract

Cloud computing security is a fundamental part of information technology planning and strategic management of digital retail operations. The infrastructure provisioning process for a cloud-based retail application is based on a series of infrastructure as code scripts, which are executed by a cloud provider on a designated cloud region, to instantiate the complete cloud setup necessary to run the application code. Emerging security trends include frameworks like coverage-driven fuzz testing and neural network-based program obfuscation for mitigating fuzzing benefits. Also, code search researchers can adopt code similarity to find the technical debt services of a large organization. Unsafe cloud computing setup procedures can result in resource exploitation, workload latencies, user data leakage, and incidents of service termination. Major cloud service providers offer an IaC toolset for building, deploying, managing, and scaling cloud applications. Configurations are based on templates, which define the cloud resources and properties to provision, and are used to invoke wrappers. In convergence with the aim of promoting the adoption of cloud technology infusing security setups for private information, a set of IaC configuration snippets is implemented for securing various components. DHCP randomly allocates four full 8-hour ports to carry out the security experiment. Only one port receives the traffic while the remaining three ports with the initial state of the primary image of the switch either remain passthrough filters or are changed to block fully the ingress traffic. Secure transport uses encryption and connections. The cache corruption attack is used to disallow non-official traffic by filtering the MAC or IPv6 address of an attacker. The cache is cleared by sending a gratuitous ARP/NA to the attacker’s linker and switching IP(s) and MAC(s).

Keywords: Amazon, Cloud security, Cloud servers, Computational modeling, Feature extraction, Feature selection, Integrated analysis, Libraries, Security, Standby systems, Support vector machines, Understanding, Virtual machine monitoring.

1. Introduction

Cloud computing is one of the most transformative technologies in the digital age. One of the most popular services in cloud computing technology is Infrastructure-as-Code (IaC). IaC enables developers to automate the cloud resource's configuration process. Cloud providers offer environment-specific configuration using dedicated command-line tools or libraries, which automatically generate resource templates. Therefore, a modern cloud computing-based application typically includes classes of Infrastructure-as-Code (IaC) files that are responsible for configuring the cloud resources, e.g., configuring the network, virtual machine, or storage. Especially in the most recent years, advancements in cloud computing technology have made the cloud a pervasive utility on retail operations infrastructure. However, cloud computing services shift most of the system's operation's duties to the consumer's responsibility, which introduces a new set of challenges, such as the potential for insecure configurations .

Cloud providers attempt to ease this configuration process by providing dedicated command line tools or libraries granting an environment-specific configuration. Cloud provisioning tools generate resources based on request configuration using provider-specific definitions. For example, referring to AWS simple storage service with the phrase "s3" followed by the bucket name and the settings requested on it would generate the expected storage resource. Such provisioning command-line tools are often used by cloud consumers to kick start the creation of resources and set their properties. Nonetheless, cloud provisioning definition is still prone to misconfiguration and security risks, as bugs can unintentionally change the desired resource settings. Recent high-impact breaches are consequences of insecure configurations, thus exposing confidential consumer data. Additionally,

shared and open-source repositories may serve as a hub of community-created resources, making it harder to ensure safe configurations coding to misuse and human errors.

Fig 1: Artificial Intelligence(AI) in Cloud Computing

1.1. Background and Significance

In order to meet the requirements and expectations of large app users, the retail industry is undergoing a significant transformation. This transformation, understood as Retail 5.0, seeks to enhance the user experience via the integration of the most suitable technologies into the infrastructure of retail environments. Through these technologies, the Smart Digital Retail Concept emerges, which offers different digital services in the physical store to create an interactive and unique experience for the end-user, ultimately stimulating purchases. Thus, it is necessary to have systems that are capable of responding quickly, efficiently, safely, and resiliently in the face of high demand, processes that have been carried out in the cloud in recent years. However, beyond the usual cloud computing approach, new trends must also be considered in order to improve the identification, tracking, and enhancement of these services.

Digital transformation plays a significant part in promoting the development of the retail industry. The realization of Digital Retail is consistent with the current trend. The emergence of blockchain further promotes the development of digitalization by solving the problem of trust between the transaction parties. The conclusion of transactions between all parties requires contracts to be written, signed and confirmed. Under the traditional transaction framework, all parties have relative trust in the transaction process. However, various factors make it impossible to completely trust the behavior of the transaction participants. Blockchain has the characteristics of decentralization, can clearly record every transaction that occurred on the chain, cannot be tampered with, and is public. On this basis, the smart contract technology developed can automatically enforce the agreed contract terms. When the trust agreement about the transaction is written into the contract, the smart contract can make the contract operational, credible, and irreversible, and further promote the development of various industries. Its application in Retail 5.0 can innovate the business model, realize the credible traceability of the producers, components, and logistics of goods. But with the large-scale application of blockchain, the threat of the combination of physical and cyber attack against blockchain cloud systems will gradually emerge.

Equ 1: Inventory Optimization Equation (Economic Order Quantity - EOQ)

$$EOQ = \sqrt{\frac{2DS}{H}}$$

Where:

- D is the annual demand for the product.
- S is the ordering cost per order.
- H is the holding cost per unit per year.

1.2. Research Objective

Although all aspects of IaC (Infrastructure as Code) crafting and the many available tools and services aiding it, current IaC provisioning tools do not automatically preclude misconfiguration and security risks. In fact, insecure IaC configuration generally translates into insecure cloud resources or infrastructure. Now most cloud service vendors provide secure configuration snippets for popular services alongside example configuration files that demonstrate their integration. Thus, the objective here is to analyze secure Terraform configuration snippets from different cloud providers and to categorize them based on the context within which they provide security improvements. This work then investigates the prevalence of these categories in a dataset of recently active open-source GitHub repositories.

2. Artificial Intelligence in Cloud Computing Security

This paper focuses on systems in the context of retail operations and points out that, from a lean perspective, appropriate infrastructure is essential in operating a smooth business. For each location, it's necessary to have the appropriate hardware – not only the actual machinery of the shop, but also supporting systems like cash registers and lighting systems. Additionally, modern shops, especially chains, are dependent on IT systems like ERP, sales data and inventory management. Each of these systems is operated via electricity, requiring properly installed electrical devices. It has to be monitored and maintained at regular intervals to identify issues before causing down times. To operate an economically successful business today, retail outlets are also often placed in busy shopping areas, which come with safety regulations that place additional demands on the infrastructure. Lastly, to maintain the lean flow of service, waste needs to be treated accordingly. There are four main concepts of Industry 4.0 that need to be implemented in the construction of the shops. Outlets are not constructed but simply leased.

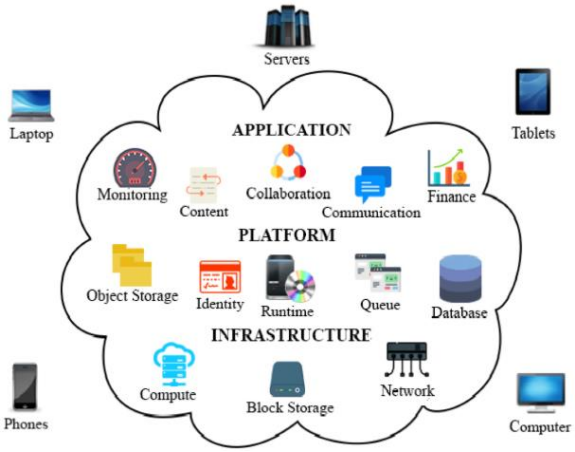

Fig 2: Cloud Computing SecurityCloud Computing Security over Smart City Networks

2.1. Overview of Artificial Intelligence

Artificial Intelligence (AI) for IT operations (AIOps) is a new initiative aimed to efficiently resolve the contradictions between AI and its deployment in retail cloud. With the surge in Artificial Intelligence capabilities being injected into the public cloud for operational purposes, how can retail smoothly transit to a cloud-centric retail method, while also remaining continuously resilient to cyber threats? There is a substantial debate within the retail organizations to push towards cloud agnosticism and enforce a cloud-neutral paradigm on infrastructure-as-code (IaC) configuration strategies, causing AI deployment to move closer to the cloud. In response, the holistic EIDA approach features an infrastructure-independent IaC cyber radar, which is capable of immersively auditing the AI-directed cloud configurations for the first instance. Through sporadically measuring the knowledge leakages in a retail's environment to the cloud, not only does EIDA manage an intelligent detection of the AI ramifications of the cloud behavior, but it can also transfigure this redacted intelligence into a blockchain-secured finely-grained retail configuration signature. In particular, the holistic EIDA model is used to reconstruct an array of the original IaC templates, swiftly revealing and forecasting the future AI-based attack patterns on, or inside, the retail cloud. A proof of concept prototype is developed to empirically evaluate EIDA with four validation mechanisms. Extensive field experiment results are reported. The achievable audit of common retail cloud security misconfigurations, depicted by the two most-widely adopted IaC configuration portfolios, and intricate AI-derived cyber intelligence leakages from them, are revealed.

2.2. Applications of AI in Cloud Computing Security

Extensive Insight Artificial Intelligence (AI) is a technology phenomenon that in recent times has managed to not only bring concerns of an impending skynet to the public but also has been met with a fair share of acknowledgment in a multitude of sectors spanning from medical research, retail, Natural Language Processing (NLP) to system and product optimizations. Thus leading a significant amount of investigation to delve into, continue and understand the potential and hazards brought on by machine learning through Artificial Intelligence (AI) and the domain specific intelligence akin to Infrastructure-as-Code (IaC) technologies in the enterprise environment.

The Information and Communication Technology (ICT) ecosystem upholds retail operations within a blended environment rendering a brick-and-click configuration. Such setups amalgamate digital Information and Communication Technology (ICT) proliferation with physical world hands-on practice giving birth to digitalized brick and mortar retail shops, pop-up shops, or temporary online forums. More precisely, a blend of cloud and edge computing technologies bristles in the retail sector, all the while honing AI, and Infrastructure-as-Code (IaC) technologies are demonstrating a blossoming inclination. Due to such structural compliances the obtuse retail mark is inadvertently a vulnerable target provoking it to malicious attacks and breach attempts . At the same time, endeavors brainstorming safeguard mechanisms are widely spread from Internet of Things (IoT) and mobile platform traceability in the retail sector, network traffic analysis, and prediction in Software Defined Networks, secure AI algorithms, and malicious traffic detection in retail operations while leveraging AI, FoG, and Blockchain technologies only mentioning a few. Network systems provision, manage and aid the overall operation of these strenuous endeavors harshly nutshelling cloud computing environments.

3. Infrastructure-as-Code (IaC) in Cloud Computing

Practicing and observing cloud computing in a retail operation is an interesting real-world situation. Cloud computing in retail operations applies to infrastructure and platform services widely. However, cloud computing security is always a concern for retail operations, because they can suffer a significant financial loss when an adversary attacks. We propose Artificial Intelligence to secure retail operations in cloud computing. In real-time, multiple networks in cloud environments, including a public cloud, a private cloud, and a retail network are protected against malicious traffic. To implement and test the proposed security environment in the real world, we use scripting tools. The entire security system is divided into three main scripts, which are found, and explanations points are provided in this paper. 13 days of experimental results are shown. From the results, the proposed Artificial Intelligence architecture in the cloud environment is successfully operating in the retail industry for 13-days production operation. There are no security breaches reported.

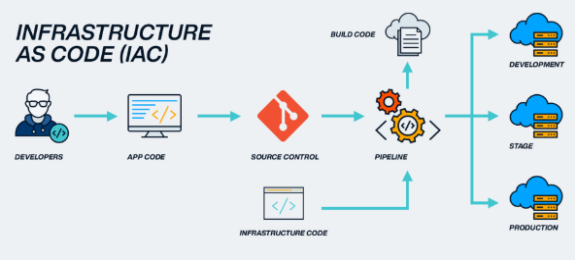

Fig 3: Infrastructure as code

3.1. Introduction to Infrastructure-as-Code

Deploying and managing cloud infrastructure at scale is cost-effective and easy with Infrastructure-as-Code (IaC) tools. In the cloud context, Infrastructure as Code is the agile process of managing and provisioning the cloud's data center using textual files, which are often, but not always, written in domain-specific languages . They describe the cloud resources and their relations, as well as the configuration constraints to be followed to create, update, and delete cloud resources.

Creating such textual files in source control grants several benefits: persistence, versioning, rollback, sharing, and reproducibility. More advanced services, such as code review, dependency management, or Continuous integration, are easily integrated due to the code nature of the files. Infrastructure as Code is then a development process benefiting from writing code principles: collaboration, code analysis, or pipeline integration. However, as cloud environments grow bigger, they become more complex and riskier in terms of security. Provisioning proper and secure cloud resources manually is a challenging task and a source of frequent human errors leading to misconfigurations which make cloud environments vulnerable to external attacks. Deploying malicious cloud resources is as easy as deploying legitimate ones. As a consequence, Infrastructure-as-Code configuration becomes a critical piece of the security of the resulting cloud setup. There should be an assurance that the Infrastructure-as-Code definitions do what they are supposed to do and no more. However, it is not uncommon for Infrastructure as Code provisioning tools to define cloud resources that are considered legitimate but automatically preclude security risks. Implementing security policies might then be a way to secure the provisioning definition. On the other hand, cloud providers provide a lot of configuration flags to tune the resources which are created. Therefore, it can be challenging to make Infrastructure as Code configurations secure in an unfamiliar cloud provider context. An empirical investigation of the adoption of best practices with secure IaC code using Terraform and different cloud providers.

3.2. Benefits of IaC in Cloud Computing

Infrastructure as Code (IaC) provisioning tools allows the design and carrying out of cloud computing infrastructures programmatically instead of confiding in manual operations. What would otherwise require numerous actions from the cloud providers' consoles can now be generated by a single script handled in a console, wrapper, Jenkins job, or GitHub Action. Cloud providers propose Terraform pieces of code to install patterns of services they deliver. The application of best practices to secure that infrastructure, such as network policy, identity management, data protection, monitoring, logging, forensics, patch and hardening, DDoS resilience, and service connectivity, will have to be done independently, regularly manually, or by dedicating tools to examine or amend that code. The paradigm of IaC might revolutionize cloud computing security for retail operations as it permits pinpointing best practices and the carrying out to a new cloud setup boils down to adapting security bookmarks in the IaC code. Make judgments on secure Terraform snippets grouping in eight discrete categories and investigate how prevalent the use of those snippets is in open-source repositories. A total of 800 secure Terraform snippets are penned down, two security analysts, two cloud practitioners, and one Ph.D. researcher in the security field on cloud computing verify that allotment of snippets to policy categories is fair, snippets are manually crafted to exhibit the track of the policy category, and two Terraform random generations are operated, independently repeated multiple times and checked automation is infeasible. On the model exposition dimension, use of meta-features to feed feature selection is described and precision by stratified coefficient of variation in the application and impact on producers' confidentiality requirements is discussed.

Equ 2: Personalized Recommendation System (Collaborative Filtering)

$$\hat{r}_{ui} = \frac{\sum_{j \in \text{similar items}(i)} sim(i,j) \cdot r_{uj}}{\sum_{j \in \text{similar items}(i)} |sim(i,j)|}$$

Where:

- $\hat{r}_{ui}$ is the predicted rating for user u on item i.
- $sim(i,j)$ is the similarity between items i and j.
- r_{uj} is the rating user u has given to item j.

4. Integration of AI and IaC in Cloud Computing Security

Traditionally, cyber defense mechanisms were static and signature-based for the most part. Nevertheless, such methods show a low efficacy today given the development of new threats, not to mention sophisticated strains of malware that change continuously. This played an important role in necessitating the continuous evolution in the infrastructure deployed in order to shield it from numerous forms of cyberattacks .

The emergence of Infrastructure-as-Code (IaC), particularly in a context of continuous integration/continuous deployment (CI/CD), provides a way to automate the deployment and changes to information systems. For developers and operations teams, IaC may simplify the design of security measures. Implementation vulnerabilities can also be identified and corrected before deployment through linter, static code analysis checkers, or security code analyzers. Security updates also become a faster process. With the creation of a pull inquiry after a security gap has been detected in the resources definition code, automatic checks will be executed within the CI/CD pipeline.

It is a widely approved notion that Artificial Intelligence (AI) will revolutionize the future of humanity and the world fundamentally. The AI applications' spectrum is broad and varies from autonomous vehicles to precision agriculture, encountered each day in online aftershops, and even in the form of social media androids.

Starting this decade, AI applications are increasingly interacting via network services harnessing the unbeatable potential and scalability of Origin computations. Unsurprisingly the dynamic distribution of these elements has seen the enterprise circling toward pioneering establishments like Google and Microsoft and spurred the explosion of services offered by them such as Amazon Web Services. At this juncture, infrastructural components are frequently outsourced as mainstream cloud services to keep pace with the state-of-the-art and ensure a high level of durability, skipping the necessity of local know-how.

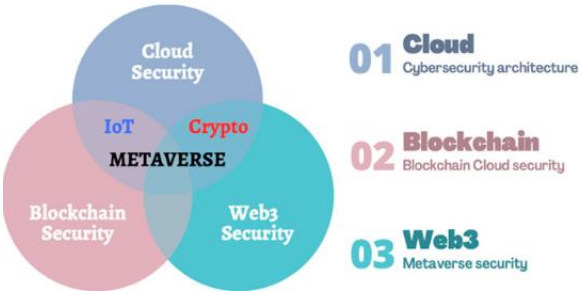

Fig 4: Integrated cybersecurity

4.1. Synergies between AI and IaC

Another promising technology is IaC, with almost USD 6 billion in increasing market size between 2017 and 2022 due to the efficiency gains it offers. Nevertheless, several issues underscore the move to and application of IaC. The increasing and changing number of configuration data, the mining libraries providing services, and the use of third-party libraries can introduce vulnerabilities to the infrastructure and threaten application integrity and confidentiality. This text looks at retail as the relevant science, focused on the security point of view. As this sector insists on providing convenience, retail requires different cloud architecture settings and aims to extract common settings. Before knowledge of cloud infrastructure, this study first classifies the Stacks and looks at the connection between back-end web service performance and DIY construction. A series of tests are then performed to mock retail operations using a specific implementation and a web platform with a welter of dynamic content. Finally, the efficiency of the back-end web service between cloud providers is taken into account.

As it enables the depicter to speak up to 40 different requirements that should be easily delivered. However, to the best of knowledge, possible threats or best practices applied to IaC code containing resources have not been previously explored. There is a fixity of locally installed IaC tools comprising security checks before making infrastructure changes. Moreover, there is a need to do cloud resources that are publicly exposed, including, without limitation, resources that allow access to everyone and services running on a computer instance.

4.2. Use Cases in Retail Operations

Retail operations is a good example of infrastructure with complex needs in having to manage a range of services. This functionality is well catered by Infrastructure as Code platforms and they give a stronger security posture at will because of the ability to version the infrastructure. As was found during the Covid-19 upshot in preparation required for remote work, sprawling infrastructure is not well constrained. Also demonstrated was a basic level of monitoring that revealed unauthorized access attempts into a cloud-based remote server that held important company data hosting. This essay will first introduce Infrastructure as Code compared to traditional Infrastructure, and explain a general purpose example of its operation. It then explores the cloud service infrastructure, and the security challenges related to them describe how Infrastructure as Code can be utilized to overcome these challenges. Finally it looks at use cases for Retail Operations, and returns to the example to apply the knowledge.

5. Case Studies and Examples

Everyday challenges to retail business operations in providing customer satisfaction are planning staffing/shift scheduling that balance with budget cost, dealing with daily uncertainty of store demands, the desirability of the product, and minimizing waste. This work demonstrates a solution framework based on reinforcement learning to address these matters. The first issue is related to a supermarket environment where visitors move along a network of several points of interest (POI), which are places of interest such as stores, promotion booths, or cashiers. The behavior of these visitors (customers) forms a complex time-dependent process conditioned upon several controllable parameters, such as the number of cashiers and the presence and location of promotion booths, which is not straightforward to model as an analytical expression . Moreover, the supermarket chain has a daily budget to incentivize clients to visit the store. So, the problem is how to choose this incentive in the most efficient way. Supermarkets Chain chooses a new exogenous demand (demand) to be selected one day in advance. Before this new demand is revealed, the chain is allowed to place promotion booths around the network, influencing the probability of customers that visit the store to either go to one of the promotion booths or

buy something. Choosing a suitable number of promotion booths around each store has a cost that must be included in the limited budget. Thus, the goal is to suggest a strategy to allocate this available budget to promotions that maximize performance of the system (profit). This supermarket environment has some similarities with the real-world problem, as a recent project showed, where the Walmart chain invested large sums to upgrade 200 stores in order to create an environment to increase in-store app usage . With the Walmart app, clients (customers) will be able to navigate the store optimally, in a similar way to how the MIP was portrayed. Incidentally, after the optimization and advice was made to the Walmart big store network, it raised discussion about the implications of using the developed strategy in practice. Therefore besides the standard problems of making a successful project compatible with a strong competitive advantage, a significant additional feature is dealing with the inherent complexity in a simple and beautiful way.

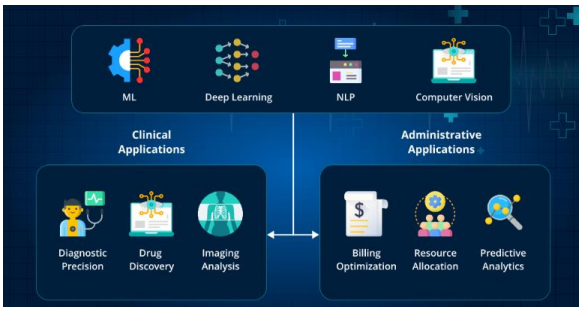

Fig 5: Integrated cybersecurity Use cases

5.1. Real-world Implementations in Retail Operations

Retail is a multifaceted environment with a great number of locations and an equally large number of security risks. Implementing cloud services in this industry would then create an additional layer of dependencies and potential vulnerabilities. On the other hand, cloud services are becoming more common and critical also in retail operations due to the significant codification and automation of routines, such as e-commerce websites, stock management systems, and accounting packages. Given the much lower complexity of the cloud service business operations when compared to retail operations, such leveraging can create opportunities for potential risks. For instance, more than 35% of the testable network connected AWS machines analyzed are poorly protected. This allows attackers to breach the build of these machines and operate within them for a long period before being detected or affect the cloud provider itself, giving access to information about other clients or disrupt the service, potentially generating losses to the retail organization.

Firstly, a study aimed at assisting the migration of retail operations to cloud while minimizing security risks presents a novel approach of gamified exercises for cloud computing teams, an approach well suited to the already killing deficit in cybersecurity personnel. Secondly, an architecture describing how this may be done is presented along with technical information about the deployability of such architecture through Infrastructure-as-Code (IaC) tools . Thirdly, various game modes are explored as an input to gamified exercises for training on AWS, Microsoft Azure, and Google Cloud, as these are the three most common cloud providers. And lastly, detailed results of the exploration of IaC tools and a suggestion of how to proceed with cloud security improvements in a gamified way. As a more technical outcome, a Terraform script is presented that automates the task of creating a central and regional virtual private cloud (VPC), transit gateways, allotment tables, route tables, and peering connections for AWS.

Equ 3: Customer Lifetime Value (CLV) Calculation

$$CLV = \frac{AOV \times F \times R}{1 + r - d}$$

Where:

- AOV is the Average Order Value.
- F is the purchase frequency.
- R is the retention rate.
- r is the discount rate (if applicable).
- d is the customer attrition rate.

6. Challenges and Future Directions

Securing cloud computing is a rapidly evolving technology, and the phenomenal growth of digitized data has empowered retailers to implement novel applications. In cloud computing, the applications are proposed to store and access pooled resources through the internet and other broadband services. However, the introduction of (IoT) devices and a blend with cloud computing enables retailers to operate more smartly. The introduction of mobile devices has heightened customer interactions. These devices have allowed consumers to shop online using cell phones and have led to more data breach attacks.

Cloud computing and IoT steadily regulate and streamline retail operations. However, if they are not secured end-to-end, they can potentially widen the attack vector for cyber crooks. Malicious attackers can intercept sensitive data, infiltrate malware, and disrupt the operations of retail systems. Critical attacks can leak out valuable information. However, securing those digitized applications is still a question. Traditional security countermeasures are unable to secure end-to-end retail operations and cloud computing systems. More substantial resources and updated systems are

required to maintain traditional security systems for detecting cyber threats. The unethical utilization of IoT and cloud resources can perform DDoS strikes. Cybercriminals can assault cloud data centers, leading to data loss and denial of service . To secure those systems, large data centers have to implement more computational resources. However, present-day retailers have the restricted budget to secure those resources.

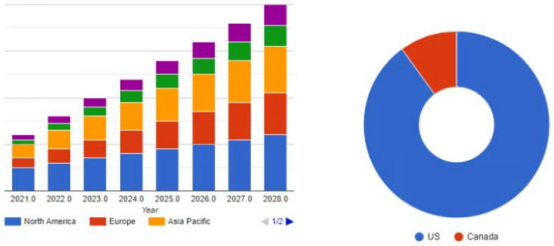

Fig : Cloud Computing Statistics to transform your Business Growth

6.1. Barriers to Adoption

Security and regulatory compliance remains one of the most important barriers to adoption of cloud computing in the retail sector. The major retailers have adopted online retailing and many have started to adopt cloud services, such as Software-as-a-Service, to support this. However, the adoption of Platforms-as-a-Service or Infrastructure-as-a-Service in more sensitive areas like stock control, cash handling or cloud Point-of-Sale systems has yet to take off. Despite the price of cloud services falling, safety concerns remain. These are centred around the fear of data loss due to corporate or state espionage, regulatory compliance – the Financial Services Sector has a legal obligation to ensure all IT systems are on UK soil – or inappropriate usage by employees. There are also misunderstandings of threats, such as a belief data is more secure behind a firewall, and a widespread belief encryption is a panacea. These concerns are not merely academic: the largest private retailer in the UK was brought to its knees by the riots, which were co-ordinated using a messaging service after intelligence suggested that encrypted services would be immune to conventional disruptive action. Recent reports indicate that attacker's methods have become highly sophisticated, using a combination of social engineering and electronic protocols; recent attacks are reported to use point-to-point encryption, which in principle is end-of-gateway-SSL-thought-to-reach-mainframe-of-vulnerability. Detection mechanisms are necessarily sophisticated, and many threats may remain undetected, particularly in cloud computing where additional vectors may be on site; a group is believed to have successfully blackmailed several retailers to the tune of a significant amount, threatening blackmail DDoS attacks otherwise.

6.2. Future Trends and Research Opportunities

Several emerging technologies such as Software Defined Networking (SDN), Network Function Virtualization (NFV), and the convergence of Information Technology (IT) and Operational Technology (OT) have become the key components for developing hybrid cloud technology. These technologies are bringing further advancements in managing networks, resources, and data centers with more flexibility and cost-efficiency. A template-based network controller connects different types of devices to automate SDN and cloud computing extension for OT through a cloud-native framework. Therefore, it is essential to develop secure, efficient, and reliable scheduling strategies for hybrid cloud applications in the aforesaid context. With growth in the retail industry, the retail business becomes more complex and distributed with connections to multiple entities in the supply chain. To achieve these objectives, Infrastructure-as-Code (IaC) using a novel Hyper-Graph Network Ecosystem (HGNE) framework is integrated with the Software Defined Cloud (SDC) to manage and reduce security threats to applications and resources in an automated and optimized fashion. This work designs schemes for auto-scaling, auto-healing, and auto-configuration using the IaC HGNE framework. Additionally, the HGNE framework helps to manage network devices for high-scale retail cloud operations. An integer linear programming model is developed for the IaC-based hypergraph network to automate and optimize scheduling strategies by considering computational, network, and economic security domains regarding retail operations utilizing hybrid clouds. Moreover, IaC declares the intended state of IT resources by using well-defined configuration files. Using the IaC-based HGNE framework, large enterprises and cloud service providers can achieve secure, efficient, and reliable retail operations and cloud service scheduling management.

7. Conclusion

Machine learning and deep learning algorithms represent the latest AI trends for 2022. They will continue to evolve and serve various industry applications. When properly applied, they can help organizations carry out their critical tasks, increase efficiency, and save money and resources. The pandemic had a decisive influence on many people who shifted from spending less time at home to going entirely remote due to the Covid-19 crisis. Therefore, they became adapted to online shopping, social media, browsing, or data communication from smartphones, tablets, and PCs. Retailers witnessed a shift in having more web traffic from physical stores to online space. The high traffic provided a playing field for hackers to exploit security vulnerabilities in a massive and distributed manner. As a result, the abuse of the Rapid Development tools, coupled with the poor adoption of the necessary security configurations, led to various high-severity risks that could have been avoided being addressed. Ensuring a well-understood deployment of the resources and capitalization on best practices is essential when the cloud is embraced for future clouds and mission-critical structures.

Infrastructure as Code (IaC) is a technology for automating the organization and provisioning of cloud infrastructure configurations. The intentions are depicted in code, offering ease of configuration management. Cloud infrastructure provisioning tools ensure the recurrent state of cloud resources according to design templates. Terraform is an IaC tool, and it explores Terraform's usage within the cloud services of different providers: Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure (AZ). We gather 287 documented Terraform secure configurations from

88 different sources, categorize them into eight groups, and employ Checkov to scan for their security vulnerabilities. We selected standard industry-recognized security policies provided by AWS, GCP, and Azure and designed 104 checks that then categorized them into five policy groups. In addition, 812 of the most "starred" active open-source GitHub repositories with Terraform were selected from each provider, and it is investigated how security policies are applied in them. Finally, this study can offer best practices for either practitioner use or service providers and a Terraform configuration secure template with the industry's acknowledged practices embedded to prevent security risks .

7.1. Summary of Key Findings

This work has revealed the findings of a research project aimed at capitalizing on the synergy between artificial intelligence powerful classifiers and the ubiquity of Infrastructure-as-Code configuration for enhancing the security of cloud-based retail operations. The outcomes presented demonstrate the potential of such synergy in leading industrial domains by shaping an automated approach to generate a high quality curated security dataset built upon the Infrastructure as Code configurations in cloud providers. Subsequently, pre-trained state-of-the-art models from the Transformers family are applied to classify said dataset into security best practices. Post-analysis extracts useful knowledge within the architecture and weights of a fine-tuned classifier ready for deployment on conditions with a resource constraint. A broader, ambitious long-term vision has also been thoroughly discussed. By automating the full processing chain, any deployment on a retail operation's job will not involve the manual intervention of a cybersecurity expert, thus drastically reducing costs. Moreover, the results can be directly used to sort out, from the myriad of configurations generated by Infrastructure-as-Code, the most critical ones, thus leading practitioners to focus on a limited and highly secure subset. As a final outcome, a Machine-Learning-as-a-Service API wrapped up of such models and their facet analysis has been made available to encourage the neuroscience of Infrastructure as Code . The dissemination of sets of manually curated best practices aligned with the widely popular Infrastructure-as-Code documentation engines is also expected to push forward the democratization of cybersecurity in cloud services among small to medium-sized retail providers.

7.2. Future Trends

Automation of predictive analytics—a part of Artificial Intelligence (AI)—has gained more limelight to solve unresolved issues and provide security threats for different applications or systems. In cloud computing, the concept of containerization alongside AI, IoT and network management were considered capable of future research directions. However, there remains a need for clear deployment options to deploy more secure and reliable (quality of service) networks. Taking these issues into account, AI is used in cloud-based networks focusing on a mechanism that can automatically encrypt the link or information (cloud service) of the provider. Virtual/extended simulators can be used to test whether the mechanism to encrypt the cloud service link has been properly secured or not .

In a retailer, the need for Cloud Data Centers (CDCs) is likely to grow during holiday seasons to temporarily increase the number of branches and customers. Therefore, most retail chains (organizations) will share the network with Telecommunication Service Providers (TSPs) in the same local area. Moreover, exposure to many cloud applications can increase security, privacy and availability risks among retail organizations and TSPs. Due to these reasons, Cloud Data Centers (CDCs) used in this environment must be secured by design. This study focuses on automating existing security mechanisms at the network edge of CDCs using Infrastructure-as-Code (IaC) and Artificial Intelligence (AI) concepts. Because of this computer architecture concept, the provider can only deploy additional cloud service links for a limited (unpredictable) amount.

8. References

[1] Kannan, S., Annapareddy, V. N., Gadi, A. L., Kommaragiri, V. B., & Koppolu, H. K. R. (2023). AI-Driven Optimization of Renewable Energy Systems: Enhancing Grid Efficiency and Smart Mobility Through 5G and 6G Network Integration. Available at SSRN 5205158.

[2] Komaragiri, V. B. The Role of Generative AI in Proactive Community Engagement: Developing Scalable Models for Enhancing Social Responsibility through Technological Innovations.

[3] Paleti, S. (2023). Data-First Finance: Architecting Scalable Data Engineering Pipelines for AI-Powered Risk Intelligence in Banking. Available at SSRN 5221847.

[4] Rao Challa, S. (2023). Revolutionizing Wealth Management: The Role Of AI, Machine Learning, And Big Data In Personalized Financial Services. Educational Administration: Theory and Practice. https://doi.org/10.53555/kuey.v29i4.9966

[5] Yellanki, S. K. (2023). Enhancing Retail Operational Efficiency through Intelligent Inventory Planning and Customer Flow Optimization: A Data-Centric Approach. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 1(1).

[6] Mashetty, S. (2023). A Comparative Analysis of Patented Technologies Supporting Mortgage and Housing Finance. Educational Administration: Theory and Practice. https://doi.org/10.53555/kuey.v29i4.9964

[7] Lakkarasu, P., Kaulwar, P. K., Dodda, A., Singireddy, S., & Burugulla, J. K. R. (2023). Innovative Computational Frameworks for Secure Financial Ecosystems: Integrating Intelligent Automation, Risk Analytics, and Digital Infrastructure. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 334-371.

[8] Motamary, S. (2022). Enabling Zero-Touch Operations in Telecom: The Convergence of Agentic AI and Advanced DevOps for OSS/BSS Ecosystems. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3833

[9] Suura, S. R., Chava, K., Recharla, M., & Chakilam, C. (2023). Evaluating Drug Efficacy and Patient Outcomes in Personalized Medicine: The Role of AI-Enhanced Neuroimaging and Digital Transformation in Biopharmaceutical Services. Journal for ReAttach Therapy and Developmental Diversities, 6, 1892-1904.

[10] Sai Teja Nuka (2023) A Novel Hybrid Algorithm Combining Neural Networks And Genetic Programming For Cloud Resource Management. Frontiers in HealthInforma 6953-6971

[11] Meda, R. (2023). Developing AI-Powered Virtual Color Consultation Tools for Retail and Professional Customers. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3577

[12] Annapareddy, V. N., Preethish Nanan, B., Kommaragiri, V. B., Gadi, A. L., & Kalisetty, S. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Venkata Bhardwaj and Gadi, Anil Lokesh and Kalisetty, Srinivas, Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing (December 15, 2022).

[13] Lakkarasu, P. (2023). Designing Cloud-Native AI Infrastructure: A Framework for High-Performance, Fault-Tolerant, and Compliant Machine Learning Pipelines. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3566

[14] Kaulwar, P. K., Pamisetty, A., Mashetty, S., Adusupalli, B., & Pandiri, L. (2023). Harnessing Intelligent Systems and Secure Digital Infrastructure for Optimizing Housing Finance, Risk Mitigation, and Enterprise Supply Networks. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 372-402.

[15] Malempati, M. (2023). A Data-Driven Framework For Real-Time Fraud Detection In Financial Transactions Using Machine Learning And Big Data Analytics. Available at SSRN 5230220.

[16] Recharla, M. (2023). Next-Generation Medicines for Neurological and Neurodegenerative Disorders: From Discovery to Commercialization. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v10i3.3564

[17] Lahari Pandiri. (2023). Specialty Insurance Analytics: AI Techniques for Niche Market Predictions. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 464-492.

[18] Challa, K. Dynamic Neural Network Architectures for Real-Time Fraud Detection in Digital Payment Systems Using Machine Learning and Generative AI.

[19] Chava, K. (2023). Integrating AI and Big Data in Healthcare: A Scalable Approach to Personalized Medicine. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v10i3.3576

[20] Kalisetty, S., & Singireddy, J. (2023). Optimizing Tax Preparation and Filing Services: A Comparative Study of Traditional Methods and AI Augmented Tax Compliance Frameworks. Available at SSRN 5206185.

[21] Paleti, S., Singireddy, J., Dodda, A., Burugulla, J. K. R., & Challa, K. (2021). Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures (December 27, 2021).

[22] Sriram, H. K. (2023). The Role Of Cloud Computing And Big Data In Real-Time Payment Processing And Financial Fraud Detection. Available at SSRN 5236657.

[23] Koppolu, H. K. R. Deep Learning and Agentic AI for Automated Payment Fraud Detection: Enhancing Merchant Services Through Predictive Intelligence.

[24] Sheelam, G. K. (2023). Adaptive AI Workflows for Edge-to-Cloud Processing in Decentralized Mobile Infrastructure. Journal for Reattach Therapy and Development Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3570

[25] Kummari, D. N. (2023). AI-Powered Demand Forecasting for Automotive Components: A Multi-Supplier Data Fusion Approach. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 1(1).

[26] Suura, S. R., Chava, K., Recharla, M., & Chakilam, C. (2023). Evaluating Drug Efficacy and Patient Outcomes in Personalized Medicine: The Role of AI-Enhanced Neuroimaging and Digital Transformation in Biopharmaceutical Services. Journal for ReAttach Therapy and Developmental Diversities, 6, 1892-1904.

[27] Balaji Adusupalli. (2022). Secure Data Engineering Pipelines For Federated Insurance AI: Balancing Privacy, Speed, And Intelligence. Migration Letters, 19(S8), 1969–1986. Retrieved from https://migrationletters.com/index.php/ml/article/view/11850

[28] Pamisetty, A. (2023). AI Powered Predictive Analytics in Digital Banking and Finance: A Deep Dive into Risk Detection, Fraud Prevention, and Customer Experience Management. Fraud Prevention, and Customer Experience Management (December 11, 2023).

[29] Gadi, A. L. (2022). Connected Financial Services in the Automotive Industry: AI-Powered Risk Assessment and Fraud Prevention. Journal of International Crisis and Risk Communication Research, 11-28.

[30] Dodda, A. (2023). AI Governance and Security in Fintech: Ensuring Trust in Generative and Agentic AI Systems. American Advanced Journal for Emerging Disciplinaries (AAJED) ISSN: 3067-4190, 1(1).

[31] Gadi, A. L. (2022). Cloud-Native Data Governance for Next-Generation Automotive Manufacturing: Securing, Managing, and Optimizing Big Data in AI-Driven Production Systems. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3758

[32] Pamisetty, A. Optimizing National Food Service Supply Chains through Big Data Engineering and Cloud-Native Infrastructure.

[33] Sriram, H. K., ADUSUPALLI, B., & Malempati, M. (2021). Revolutionizing Risk Assessment and Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks.

[34] Chakilam, C. (2022). Integrating Machine Learning and Big Data Analytics to Transform Patient Outcomes in Chronic Disease Management. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v9i3.3568

[35] Koppolu, H. K. R. (2021). Leveraging 5G Services for Next-Generation Telecom and Media Innovation. International Journal of Scientific Research and Modern Technology, 89–106. https://doi.org/10.38124/ijsrmt.v1i12.472

[36] Sriram, H. K. (2022). Integrating generative AI into financial reporting systems for automated insights and decision support. Available at SSRN 5232395.

[37] Paleti, S., Burugulla, J. K. R., Pandiri, L., Pamisetty, V., & Challa, K. (2022). Optimizing Digital Payment Ecosystems: Ai-Enabled Risk Management, Regulatory Compliance, And Innovation In Financial Services. Regulatory Compliance, And Innovation In Financial Services (June 15, 2022).

[38] Malempati, M., Pandiri, L., Paleti, S., & Singireddy, J. (2023). Transforming Financial And Insurance Ecosystems Through Intelligent Automation, Secure Digital Infrastructure, And Advanced Risk Management Strategies. Jeevani, Transforming Financial And Insurance Ecosystems Through Intelligent Automation, Secure Digital Infrastructure, And Advanced Risk Management Strategies (December 03, 2023).

[39] Karthik Chava. (2022). Harnessing Artificial Intelligence and Big Data for Transformative Healthcare Delivery. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 502–520. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11583

[40] Challa, K. (2023). Optimizing Financial Forecasting Using Cloud Based Machine Learning Models. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3565

[41] Pandiri, L., Paleti, S., Kaulwar, P. K., Malempati, M., & Singireddy, J. (2023). Transforming Financial And Insurance Ecosystems Through Intelligent Automation, Secure Digital Infrastructure, And Advanced Risk Management Strategies. Educational Administration: Theory and Practice, 29 (4), 4777–4793.

[42] Recharla, M., & Chitta, S. AI-Enhanced Neuroimaging and Deep Learning-Based Early Diagnosis of Multiple Sclerosis and Alzheimer's.

[43] Pamisetty, A., Sriram, H. K., Malempati, M., Challa, S. R., & Mashetty, S. (2022). AI-Driven Optimization of Intelligent Supply Chains and Payment Systems: Enhancing Security, Tax Compliance, and Audit Efficiency in Financial Operations. Tax Compliance, and Audit Efficiency in Financial Operations (December 15, 2022).

[44] Kaulwar, P. K. (2022). Securing The Neural Ledger: Deep Learning Approaches For Fraud Detection And Data Integrity In Tax Advisory Systems. Migration Letters, 19, 1987-2008.

[45] Lakkarasu, P. (2023). Generative AI in Financial Intelligence: Unraveling its Potential in Risk Assessment and Compliance. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 241-273.

[46] Gadi, A. L., Kannan, S., Nanan, B. P., Komaragiri, V. B., & Singireddy, S. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization. Universal Journal of Finance and Economics, 1(1), 87-100.

[47] Meda, R. (2022). Integrating IoT and Big Data Analytics for Smart Paint Manufacturing Facilities. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3842

[48] Nuka, S. T., Annapareddy, V. N., Koppolu, H. K. R., & Kannan, S. (2021). Advancements in Smart Medical and Industrial Devices: Enhancing Efficiency and Connectivity with High-Speed Telecom Networks. Open Journal of Medical Sciences, 1(1), 55-72.

[49] Suura, S. R. (2022). Advancing Reproductive and Organ Health Management through cell-free DNA Testing and Machine Learning. International Journal of Scientific Research and Modern Technology, 43–58. https://doi.org/10.38124/ijsrmt.v1i12.454

[50] Kannan, S. The Convergence of AI, Machine Learning, and Neural Networks in Precision Agriculture: Generative AI as a Catalyst for Future Food Systems.

[51] Implementing Infrastructure-as-Code for Telecom Networks: Challenges and Best Practices for Scalable Service Orchestration. (2021). International Journal of Engineering and Computer Science, 10(12), 25631-25650. https://doi.org/10.18535/ijecs.v10i12.4671

[52] Singireddy, S. (2023). AI-Driven Fraud Detection in Homeowners and Renters Insurance Claims. Journal for Reattach Therapy and Development Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3569

[53] Mashetty, S. (2022). Innovations In Mortgage-Backed Security Analytics: A Patent-Based Technology Review. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3826

[54] Rao Challa, S. (2023). Artificial Intelligence and Big Data in Finance: Enhancing Investment Strategies and Client Insights in Wealth Management. International Journal of Science and Research (IJSR), 12(12), 2230–2246. https://doi.org/10.21275/sr231215165201

[55] Paleti, S. (2023). Trust Layers: AI-Augmented Multi-Layer Risk Compliance Engines for Next-Gen Banking Infrastructure. Available at SSRN 5221895.

[56] Pamisetty, V., Pandiri, L., Annapareddy, V. N., & Sriram, H. K. (2022). Leveraging AI, Machine Learning, And Big Data For Enhancing Tax Compliance, Fraud Detection, And Predictive Analytics In Government Financial Management. Machine Learning, And Big Data For Enhancing Tax Compliance, Fraud Detection, And Predictive Analytics In Government Financial Management (June 15, 2022).

[57] Komaragiri, V. B. (2023). Leveraging Artificial Intelligence to Improve Quality of Service in Next-Generation Broadband Networks. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3571

[58] Kommaragiri, V. B., Preethish Nanan, B., Annapareddy, V. N., Gadi, A. L., & Kalisetty, S. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Venkata Narasareddy and Gadi, Anil Lokesh and Kalisetty, Srinivas.

[59] Annapareddy, V. N. (2022). Integrating AI, Machine Learning, and Cloud Computing to Drive Innovation in Renewable Energy Systems and Education Technology Solutions. Available at SSRN 5240116.

[60] Komaragiri, V. B. (2022). Expanding Telecom Network Range using Intelligent Routing and Cloud-Enabled Infrastructure. International Journal of Scientific Research and Modern Technology, 120–137. https://doi.org/10.38124/ijsrmt.v1i12.490

[61] Vamsee Pamisetty. (2020). Optimizing Tax Compliance and Fraud Prevention through Intelligent Systems: The Role of Technology in Public Finance Innovation. International Journal on Recent and Innovation Trends in Computing and Communication, 8(12), 111–127. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11582

[62] Paleti, S. (2023). AI-Driven Innovations in Banking: Enhancing Risk Compliance through Advanced Data Engineering. Available at SSRN 5244840.

[63] Srinivasa Rao Challa,. (2022). Cloud-Powered Financial Intelligence: Integrating AI and Big Data for Smarter Wealth Management Solutions. Mathematical Statistician and Engineering Applications, 71(4), 16842–16862. Retrieved from https://philstat.org/index.php/MSEA/article/view/2977

[64] Srinivasa Rao Challa,. (2022). Cloud-Powered Financial Intelligence: Integrating AI and Big Data for Smarter Wealth Management Solutions. Mathematical Statistician and Engineering Applications, 71(4), 16842–16862. Retrieved from https://philstat.org/index.php/MSEA/article/view/2977

[65] Someshwar Mashetty. (2020). Affordable Housing Through Smart Mortgage Financing: Technology, Analytics, And Innovation. International Journal on Recent and Innovation Trends in Computing and Communication, 8(12), 99–110. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11581

[66] Singireddy, S. (2023). Reinforcement Learning Approaches for Pricing Condo Insurance Policies. American Journal of Analytics and Artificial Intelligence (ajaai) with ISSN 3067-283X, 1(1).

[67] Transforming Renewable Energy and Educational Technologies Through AI, Machine Learning, Big Data Analytics, and Cloud-Based IT Integrations. (2021). International Journal of Engineering and Computer Science, 10(12), 25572-25585. https://doi.org/10.18535/ijecs.v10i12.4665

[68] Chava, K., Chakilam, C., Suura, S. R., & Recharla, M. (2021). Advancing Healthcare Innovation in 2021: Integrating AI, Digital Health Technologies, and Precision Medicine for Improved Patient Outcomes. Global Journal of Medical Case Reports, 1(1), 29-41.

[69] Raviteja Meda. (2021). Machine Learning-Based Color Recommendation Engines for Enhanced Customer Personalization. Journal of International Crisis and Risk Communication Research , 124–140. Retrieved from https://jicrcr.com/index.php/jicrcr/article/view/3018

[70] Nandan, B. P., & Chitta, S. (2022). Advanced Optical Proximity Correction (OPC) Techniques in Computational Lithography: Addressing the Challenges of Pattern Fidelity and Edge Placement Error. Global Journal of Medical Case Reports, 2(1), 58-75.

[71] Phanish Lakkarasu. (2022). AI-Driven Data Engineering: Automating Data Quality, Lineage, And Transformation In Cloud-Scale Platforms. Migration Letters, 19(S8), 2046–2068. Retrieved from https://migrationletters.com/index.php/ml/article/view/11875

[72] Kaulwar, P. K. (2022). Data-Engineered Intelligence: An AI-Driven Framework for Scalable and Compliant Tax Consulting Ecosystems. Kurdish Studies, 10 (2), 774–788.

[73] Malempati, M. (2022). Transforming Payment Ecosystems Through The Synergy Of Artificial Intelligence, Big Data Technologies, And Predictive Financial Modeling. Big Data Technologies, And Predictive Financial Modeling (November 07, 2022).

[74] Recharla, M., & Chitta, S. (2022). Cloud-Based Data Integration and Machine Learning Applications in Biopharmaceutical Supply Chain Optimization.

[75] Lahari Pandiri. (2022). Advanced Umbrella Insurance Risk Aggregation Using Machine Learning. Migration Letters, 19(S8), 2069–2083. Retrieved from https://migrationletters.com/index.php/ml/article/view/11881

[76] Chava, K. (2020). Machine Learning in Modern Healthcare: Leveraging Big Data for Early Disease Detection and Patient Monitoring. International Journal of Science and Research (IJSR), 9(12), 1899–1910. https://doi.org/10.21275/sr201212164722

[77] Data-Driven Strategies for Optimizing Customer Journeys Across Telecom and Healthcare Industries. (2021). International Journal of Engineering and Computer Science, 10(12), 25552-25571. https://doi.org/10.18535/ijecs.v10i12.4662

[78] Dwaraka Nath Kummari,. (2022). Machine Learning Approaches to Real-Time Quality Control in Automotive Assembly Lines. Mathematical Statistician and Engineering Applications, 71(4), 16801–16820. Retrieved from https://philstat.org/index.php/MSEA/article/view/2972

[79] Chaitran Chakilam. (2022). AI-Driven Insights In Disease Prediction And Prevention: The Role Of Cloud Computing In Scalable Healthcare Delivery. Migration Letters, 19(S8), 2105–2123. Retrieved from https://migrationletters.com/index.php/ml/article/view/11883

[80] Adusupalli, B. (2023). DevOps-Enabled Tax Intelligence: A Scalable Architecture for Real-Time Compliance in Insurance Advisory. Journal for Reattach Therapy and Development Diversities. Green Publication. https://doi. org/10.53555/jrtdd. v6i10s (2), 358.

[81] Pamisetty, A. (2023). Cloud-Driven Transformation Of Banking Supply Chain Analytics Using Big Data Frameworks. Available at SSRN 5237927.

[82] Gadi, A. L. (2021). The Future of Automotive Mobility: Integrating Cloud-Based Connected Services for Sustainable and Autonomous Transportation. International Journal on Recent and Innovation Trends in Computing and Communication, 9(12), 179-187.

[83] Pandiri, L., & Chitta, S. (2022). Leveraging AI and Big Data for Real-Time Risk Profiling and Claims Processing: A Case Study on Usage-Based Auto Insurance. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3760

[84] Innovations in Spinal Muscular Atrophy: From Gene Therapy to Disease-Modifying Treatments. (2021). International Journal of Engineering and Computer Science, 10(12), 25531-25551. https://doi.org/10.18535/ijecs.v10i12.4659

[85] Adusupalli, B., Singireddy, S., Sriram, H. K., Kaulwar, P. K., & Malempati, M. (2021). Revolutionizing Risk Assessment and Financial Ecosystems with Smart Automation, Secure Digital Solutions, and Advanced Analytical Frameworks. Universal Journal of Finance and Economics, 1(1), 101-122.

[86] Operationalizing Intelligence: A Unified Approach to MLOps and Scalable AI Workflows in Hybrid Cloud Environments. (2022). International Journal of Engineering and Computer Science, 11(12), 25691-25710. https://doi.org/10.18535/ijecs.v11i12.4743

[87] Data Engineering Architectures for Real-Time Quality Monitoring in Paint Production Lines. (2020). International Journal of Engineering and Computer Science, 9(12), 25289-25303. https://doi.org/10.18535/ijecs.v9i12.4587

[88] Rao Suura, S. (2021). Personalized Health Care Decisions Powered By Big Data And Generative Artificial Intelligence In Genomic Diagnostics. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v7i3.3558

[89] Kannan, S., & Saradhi, K. S. Generative AI in Technical Support Systems: Enhancing Problem Resolution Efficiency Through AIDriven Learning and Adaptation Models.

[90] Kurdish Studies. (n.d.). Green Publication. https://doi.org/10.53555/ks.v10i2.3785

[91] Srinivasa Rao Challa,. (2022). Cloud-Powered Financial Intelligence: Integrating AI and Big Data for Smarter Wealth Management Solutions. Mathematical Statistician and Engineering Applications, 71(4), 16842–16862. Retrieved from https://www.philstat.org/index.php/MSEA/article/view/2977

[92] Paleti, S. (2022). The Role of Artificial Intelligence in Strengthening Risk Compliance and Driving Financial Innovation in Banking. International Journal of Science and Research (IJSR), 11(12), 1424–1440. https://doi.org/10.21275/sr22123165037

[93] Kommaragiri, V. B., Gadi, A. L., Kannan, S., & Preethish Nanan, B. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization.