International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

Modernizing Enterprise Systems Using Intelligent Microservices and Google Cloud Platform

Amit Rajula

Independent Researcher, USA

ABSTRACT: Enterprise modernization is already being viewed as a strategic concern and organizations are panhandling to change monolithic applications with resilient, intelligent and scalable cloud-individualization systems, which will respond and adapt to changing business needs. Traditional enterprise systems would be less scaled, expensive to maintain, their deployment process slow and they cannot be integrated with the new artificial intelligence (AI) inventions. The framework presented in this paper is an Intelligent Microservices Modernization Framework (IMMF) which was designed on Google Cloud Platform (GCP) to refine the legacy enterprising apps into a new format of smarter and more resilient cloud-native services, in modules. This architecture features microservices based on API, Kubernetes containers and event-based communication via Pub/Sub, a serverless processing engine using Cloud Functions/Cloud Run, AI-powered analytics as a component of Vertex AI, intelligent monitoring as a component of Cloud Operations Suite, identities and access control, CI/CD automation, and central observability. The framework also adds predictive autoscaling, anomaly detection, smart workload orchestrator and autoscale fault recovery to enhance the reliability and efficiency of the services. It is designed to be more scalable to applications that can be deployed and optimized based on the resource needs it has a more secure nature, a greater interoperability and business continuity, simplifies and minimises operational complexities, and costs less to operate due to the combination of the microservices architecture and cloud-native infrastructure, AI enhanced operation intelligence. The study provides a summary of the overall reference of the architecture of the enterprise interested in accelerating the digital transformation by smartly modernizing its cloud-native through Google Cloud Platform.

KEYWORDS: Enterprise Modernization, Intelligent Microservices, Google Cloud Platform (GCP), Cloud-Native Architecture, Kubernetes, Vertex AI, DevOps Automation

I. INTRODUCTION

The burning effect of the digital technologies is that the current generation of businesses has altered a significant design, deployment and management of business applications. Digital transformations are gaining momentum at an organization in all industries as organisations gain the aspiration to make operation, customer relations, scalability and resiliency of business more efficient. However, majority of businesses continue to utilize the monolithic systems that had been created decades ago to work with comparatively fixed business procedures. Despite the effectiveness of these systems over the years, cases where they fail to cope up with the demands of the modern business world that is dynamic and requires quick innovation, continuous application, real time analytics and seamless integration with cloud service are not uncommon. The growing expectation of the customer and the global growth of businesses need high availability, elasticity, security and smart business decision making in enterprise applications as well as reducing the cost of operations and infrastructure has compelled the use of applications that have the ability to achieve a high level of elasticity, availability, security, and smart decision-making.

With the older, monolithic structures, all business functionality is installed as one deployable application, developing, testing, deploying and maintaining the system becomes extremely complicated as it becomes more complex. Even one modification to a single module is also likely to cause a red deployment of the whole application which will cause downtime and slowness of innovation. Moreover, all monoliths are not scalable as in most cases you need to replicate the whole stack of the application because only a small number of services run more workloads, not efficiently using the resources available and other services increase the cost of the infrastructure. Absorption of new technology, e.g., artificial intelligence (AI), machine learning (ML), Internet of Things (IoT), big data analytics and real-time event processing is further complicated by the inability of monolithic architecture to be easily adapted to new emerging technologies due to lack of modularity and flexibility.

One of most treasured ways of modernizing enterprise systems is by employing the microservices architecture, which consists of decomposing the big density monolithic applications to small and un-bounded loosely coupled services. The microservices handle a particular business capability and communicate with other services via simple APIs or event-

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

based messaging services. It is a modular design such that every one of the services may be created, tried, launched, increased and maintained, without influencing the entire application. Development teams will be able to take on agile practices, improve software development processes, mitigate the risk of software deployments and enhance system resilience with the assistance of isolating faults. Since there is flexibility (or choice) of the most appropriate technologies to employ by different business functions since each service can be done using the most suitable programming language, database and technology stack, organizations can attain a lot of flexibility in terms of selection of the most suitable technologies.

Its emergence in the growing use of cloud computing has also contributed to modernization of enterprise due to availability of a highly scalable, reliability and cost effective infrastructure. Cloud-native development enables companies to develop purpose-written applications to run in a distributed computing environment, and builds managed services that are built on top of it to deploy this operational overhead much lower as compared to traditional data centers. Google Cloud Platform (GCP) is one of the most popular cloud service providers with versatile ecosystem of cloud-native services enabling smart fastening of the enterprise modernization. The Google Kubernetes Engine (GKE), Cloud Run, Cloud Functions, Pub/Sub, Cloud SQL, Firestore, BigQuery, Vertex AI, Cloud Build, Artifact Registry, Cloud Monitoring and Cloud Logging services allow enterprises to create highly resilient and large-scale enterprise applications and to dramatically simplify the complexity of running and managing infrastructure.

The technologies of containerization have fostered the use of cloud-native applications. Containers are applications and assemblages of runtime dependencies, that is, they can always be successfully deployed in any development, testing and production environment. The orchestration of containerized workloads, the automatic deployment, the automatic discovery of the service, rolling updates, self healing and load balancing and horizontal autoscaling are some of the aspects that Kubernetes has become the new standard in the industry. An alternative that would simplify the management of Kubernetes is Google Kubernetes engine, which provides a fully-managed Kubernetes and the enterprise will be able to build applications instead of maintaining the infrastructure. Combined with Cloud Run to offer serverless container deployments and Cloud Functions to offer event-driven processing, GCP can be used to help an enterprise come up with highly efficient hybrid application architectures, which can be dynamically scaled to meet changing workloads.

AI has become a new component of an enterprise system. AI is becoming part of the operations of businesses more fundamentally, as an attempt to automatize decisions, maximize resource usage, identify anomalies, anticipate system failures, and tailor customer experiences, rather than simply a second-order tool. The operational data of the distributed services, infrastructure components, user interactions and business transactions are continuously collected by smart enterprise applications. These classes of data streams are modeled to identify performance bottlenecks, predict resource needs, workloads how to place them optimally, security threats detected, and remedies prescribed, due to machine learning models. Google Vertex AI provides a suite to create, train, deploy, and manage machine learning that can be deployed to cloud applications, and can be easily incorporated into enterprise applications to help an organization go beyond reactive operations and process into predictive and autonomous operations.

Another essential requirement in such a distributed micro services environment that has emerged is observability. Microservices do not contribute to centralized application monitoring compared to monolithic systems, and leave the logs, metrics, traces and events to flow in many independent services. Detecting performance degradation, debugging failures, following service dependencies and observing service-level objectives (SLOs) are prerequisites of monitors and observability. Google cloud operations suite is a collection, with monitoring, logging, distributed tracing, profiling and alerting services all provided as one platform, to allow realtime visibility of a user to a complex enterprise environment. Other AI-based surveillance-based apps could also operate predictive maintenance to anticipate an abnormal behavior and prevent it before it occurs, disrupting the service delivery.

Security is among the largest challenges in regards to modernizing a business. With the ever-growing dispersion of apps, inter-microservice communication becomes much harder to secure and identities, sensitive data, and regulatory compliance are much harder. Google Cloud Platform provides complete security features that can be inclusive of Identity and Access Management (IAM), Secret Manager, Cloud Armor, Web Application Firewall (WAF), encrypting both data and networkwide, Binary Authorization, and Security Command Center, and per-organization-wide policy. The concepts of zero trust of security also provides better protection against intruders in which users, devices and workloads are authenticated prior to gaining access to resources.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

CI/CD pipelines are relevant as they help to accelerate the provision of the software in a cloud-native platform. The automated build, testing, containerization and vulnerability scanning, deployment and roll back would improve the quality of the software but successful deployment would be achieved with a minimum involvement of human labor and minimum roll back challenges. The fully automated Devops to roll out features quickly and encourage continuous improvements required of organisations to roll out can be developed using artifact Registry, Cloud Build, Cloud Deploy and Git-based repositories. Along with the infrastructure-as-code and policy automation, organizations could roll out infrastructure at a very high degree of consistency, reproducibility and security among various environments.

All these advantages of cloud-native technologies notwithstanding, the process of implementing the enterprise modernization is a complicated and difficult one. The migrations of their legacy systems, de-composing of their services, intra-service communications, distributed transactions, data consistency, governance, performance performance optimization, monitoring operations, enforcing security and cost management are all considered some of the most prevalent issues organizations are grappling with. Devoid of a modernization strategy, migration initiatives can bring about an unwanted level of complexity, service dependencies, operational risks, possibly augmented maintenance costs. This, further, has spurred an increasing demand of wholesome contemporary models of modernization that are able to bring along architectural brilliantness, cloud-native, and intensive automation, intelligent AI-driven operation, security governance, and persistent delivery, into a series of aggregated enterprise transformation technique.

To solve these challenges, the proposed paper offers one Intelligent Microservices Modernization Framework (IMMF) with Google cloud platform as the solution. The architecture weaves together the microservice architecture, orchestration of containers and serverless computing, API management, event-driven communications, artificial intelligence based analytics, intelligent monitoring, automated scaling, automated DevOps and end-to-end security services within a cloud-native ecosystem. Using both modules-based software design and smart operational management as an exploitative tool, the framework will be helpful in enhancing the scalability, resilience, fault tolerance, agility in deploying, resource efficiency, security, and business continuity. The given architecture implies the enterprises a real roadmap on their way towards the modernisation of the outdated enterprise systems and the utilisation of the comprehensive platform of the services of the Google Cloud as well as artificially intelligent to allow the organisations to proceed with the digital transformation process in the ever-growing competitive business environments.

II. LITERATURE REVIEW

Enterprise systems modernization is now one of the hottest research agendas due to the increased demand to possess scalable, resilient and intelligent software platforms able to deliver digital transformation. Cloud-native microservices on popular cloud computing systems are replacing monolithic-based systems. Recent studies have been on component imbedding of microservices, container treatment, artificial intelligence (AI), devops and cloud-native infrastructure to enhance scalability of applications, business rapidly and competitiveness.

A very detailed manual on cloud and enterprise architecture and application design was given by Goniwada [1]. The paper has discussed how monoliths may be turned into modular applications which are executed on a software based and container based cloud, kubernetes, service meshes, and event based communication. The author emphasized that modernization of enterprises needs to embrace adoption of distributed architecture with capability to be deployed independently, scaled continuously, have automated monitoring, and deployable resource handling. The task had also been troubled with the importance of aligning the demands and principles of cloud-native architecture with the requirements of the enterprise-wide governance, security and automation to create hypertensive robust and application of business programs.

Balalaie et al. [2] investigated the way of how enterprise systems could be migrated to utilize the DevOps practice to shift them out of monolithic systems to microservices based on the cloud. Their findings revealed that the implementation of the applications, divided into loosely-coupled services, leads to faster deployment, greater software maintenance, fault and coordination isolation as well as isolation of faults in the organization. The other finding that the authors could arrive at is that the continuous integration and continuous deployment (CI/CD) pipelines minimise the risk associated with deployments besides speeding up software deliveries. The work was one of the pioneer utilization of microservices architecture and DevOps methods that may be useful in the modernization efforts of enterprises.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

Kratzke and Quint [3] presented the map of a mapping exercise of cloud-native applications after decade of experience in cloud computing development. They could infer conclusions regarding the result of the plethora of studies and found cloud-native applications to be those systems with the following characteristics: containerization, elasticity, continuous delivery, service independence, and automated management of the infrastructure. The researchers have discovered that cloud-native architecture enables business to rapidly adapt to evolving business needs as it improves the reliability and operational efficiency of the applications. However, some challenges related to complexity of distributed systems, monitoring, communication between the services and operational governance were also provided by the authors.

The reference model of Clou NS (Cloud-native Stack) developed by Kratzke and Peinl [4] is aimed at assisting the enterprise architects during the process of changing the enterprise into the cloud. This framework divides cloud-native systems, into several layers of architecture which include infrastructure, container runtime, orchestration, application services and business functionality. The reference architecture is a formal attitude to architecturing enterprise applications and their realisation is scaled as well as interoperable, portable and maintainable. The proposed layered solution creates a simplification of the migration planning, and allows the organisations to modernise the old-windered software system in systematically ordered model with utilisation of the standardized cloud-native applications.

The architectural concepts of the cloud software engineering that were reviewed by Pahl, Jamshidi and Zimmermann [5] include those of the core concepts. In it, they have identified the following main attributes of the cloud-native systems, modularity, loose coupling, elasticity, scalability, fault tolerance, service autonomy, and an API-based communication. Even the authors provided an explanation of the significance of distributed data management, resiliency engineering, security-by-design and continuous monitoring of present-day enterprise application. They extensively feature in their architecture needs to develop a scaled distributed systems that are then run on the public cloud solutions.

After becoming aware of the increased usage of the term microservice, Pahl and Jamshidi [6] have undertaken one of the first attempts to have a systematic mapping study that is specifically oriented to microservice research. Their review categorized literature according to architectural design, service decomposition, protocols communications, deployment models, and monitoring techniques and performance appraisal. The article has demonstrated the greatest advantages of autonomous deployment, decentralized leadership, and lightweight interaction as the main advantages of microservices and has found the problem of distributed transactions, service introduction, debugging and complicatedness of operations. The findings were a credible source of information on fast modernization process of the enterprises.

Bakshi [7] described the approach of using software engineering based on using micro services-based architectures as well. The services encompass autonomously deployed services, API gateway, containerization, service registries and asynchronous communication protocols which were assessed in the paper. The author could gain some conclusion about the fact that microservices contribute to the flexibility, scalability and maintainability of the software, as well as enable organizations to adopt agile practices of development. The paper has however underscored the role of comprehensively monitoring, deploying resources of security and orchestration to be able to effectively control the more spread out enterprise landscapes.

With Kubernetes now being the most popular orchestrator tool of cloud based applications, Dobies and Wood [8] postulated Kubernetes Operators as an emergent sophisticated tool of automation in order to manage complicated workloads in enterprises. They demonstrated with their work how the operators can be extended with domain-specific operational expertise in software controllers which can be used to automate the deployment, scaling, backup, recovery and lifecycle management. The authors claimed that automation based on operators dramatically lowers the administration overhead and increases the reliability of applications and consistency of operations in a production cloud environment.

Brikman [9] has concentrated on Infrastructure as Code (IaC) which uses Terraform to provide an automated method of delivering infrastructure to the cloud. The types of deployable virtual machines, container clusters, networking, storage, identity management and cloud services that are presented in the book have such a form of declarative configuration files. The study demonstrated that IaC can help with a consistent deployment, manage versions, scale infrastructure and process recovery and minimize configuration errors through a manual administration. Ever since, Terraform has proven to be among the most utilized toolsets of enterprise DevOps pipelines.

Increasingly, artificial intelligence has become a part of the enterprise cloud platforms. Bisong [10] announced Kubeflow and Kubeflow pipelines, end-to-end machine learning lifecycle management systems, that are managed on

|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|
DOI: 10.15662/IJSRAT.2023.0602002

Google Cloud Platform. The paper described the capability of automated Kubernetes-deployed distributed machine learning workflows to offer the tools to scale up model training, deployment, monitoring, and continual retraining. AI pipeline orchestration with cloud-native infrastructure offers business organizations with decision support and machine learning operations (MLOps).

Curious about exploring the principle of Kubernetes Operators as a smart process to manage cloud-native applications, Chemashkin and Drobintsev [11] worked out the idea of Kubernetes automation. Through their work they revealed how operators are continuously monitoring the well-being of clusters, failures are detected, auto recovery is initiated and application implemented in line with the operational policies. Kubernetes Operators can improve the operational reliability, fault tolerance and operational efficiency by incorporating operational intelligence into orchestration systems without involving considerable level of manual intervention.

One of the most complicated problems of the distributed clouds in the cloud-native applications is state management. When examining how to deal with application state in micro-services distributed in a manner to ensure consistency, Szalay et al. [12] undertook the aspects of scalability and fault tolerance. The contents of their work concerned stateful containers, distributed databases, persistent storage and checkpointing and synchronization technique methods that instill confidence in running enterprise workloads on Kubernetes. The authors reminded how the state needs to be managed to deliver a business critical cloud native application which needs to be highly available and with the nature of transactional integrity.

Hendrickson et al. [13] regard OpenLambda as an initial serverless computing framework, which is designed to support Function-as-a-Service (FaaS) applications. Their paper has demonstrated that serverless infrastructures as compared to the traditional infrastructure approach are highly resourceful in the management of infrastructures through scaling out of the computing resources automatically in response to the relevant event taking place. The proposed implementation pattern improves the scalability, resource usage and easiness of operations and enables the developers to focus more on business logic. Since serverless has become a noticeable characteristic of the modern cloud environment in an enterprise, cloud functions (e.g., Google Cloud Functions and Cloud Run) and these cloud services have become key players.

Moreno, Gonzalez and Viedma [14] introduced an idea of such enterprise architecture that encompasses the use of big data analytics and artificial intelligence into cloud computing incidences. One of the designs was their illustration of cloud-native data platform featuring scalable data storage, distributed analytics, machine learning, and real time information processing to support smart business decisions. The authors have found that the competitiveness of organizations raised to the high level can be attained through AI and cloud infrastructure implementation since it may become possible to introduce predictive analytics and conduct intelligent automation, as well as make data-driven strategies.

Lastly, Dinh-Tuan et al. [15] proposed a court design of a microservices-based architecture named the Maia, which has been scaled to the needs of the industrial data analytics applications. The architecture proposed included the use of distributed data collection, scalable analytics service, and containerized deployment and communication using API to scale industrial workloads effectively. The framework indicated that the microservices architecture can increase the scalability, modularity, maintainability and real-time data processing of the system, as well as simplify the integration with technologies of artificial intelligence and cloud computing.

In general terms, the literature reviewed shows that there has been a lot of advancement in the field of the modernization of the enterprise cloud-native, according to microservices, Kubernetes orchestration, automation of the DevOps processes, the Infrastructure as Code of serverless computing and artificial intelligence-supported cloud platform. However, the new researches focus mainly on these technologies separately. Minimal literature has given such a unified framework into which such options as smart microservices, AI-driven operational management and Kubernates orchestration, DevOps automation, serverless services and the Google Cloud Platform are united within a single modernization of an enterprise. The gap this latter paper fills is the proposal of an Intelligent Microservices Modernization Framework (IMMF) that brings these complimentary technologies together in such a way that scalable, resilient, secure and intelligent enterprise systems are deplored on Google Cloud Platform.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

III. INTELLIGENT MICROSERVICES MODERNIZATION FRAMEWORK (IMMF)

The change involved in moving enterprise computing has accelerated the dumping of monolithic applications into cloud-native ecosystems capable of theoretically rendering it scalable, resilient and automated in addition to making intelligent decisions. Despite the widespread integration of microservices in architecture practices, most organizations are still faced with issues that relate to migrating legacy applications, orchestrating services, monitoring operations, overseeing security, optimizing resources, and integrating with artificial intelligence (AI). These issues will make even more complicated the process of modernization of enterprises, as well as make it harder to use the possibilities of cloud computing by organizations. As a solution to these shortcomings, this paper suggests an Intelligent Microservices Modernization Framework (IMMF) that uses Google Cloud Platform (GCP). The microservices that are proposed to be deployed on a cloud, container orchestration, serverless computing, Artificial Intelligence-based analytics, automated processes offered by the DevOps, smart monitoring, and cloud security are incorporated in a single framework, culminating in the Christianization of the enterprise.

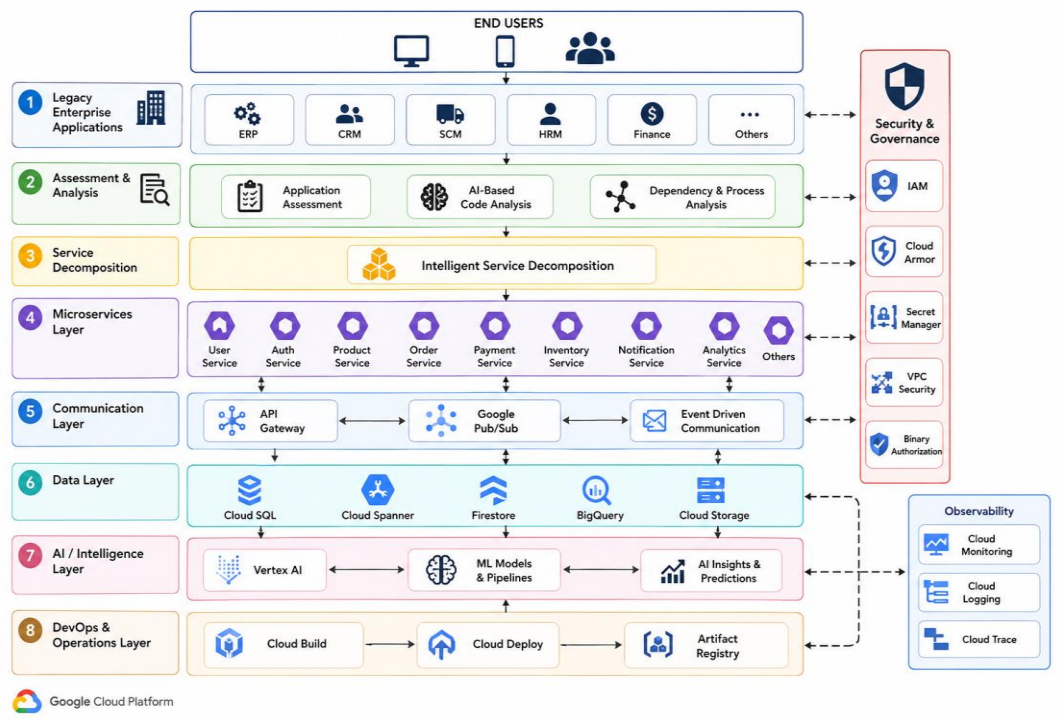

Figure 1- Overall Intelligent Microservices Modernization Framework (IMMF) Architecture

The proposed architecture will have eight interacting layers that sustain the entire life cycle of business applications such as modernization, deployment, coordination, monitoring, optimization and upgrade. All layers have a specific set of functions and interact safely with the neighbouring layers using standardised APIs and event-based messaging services. The commonality of these layers offers intelligent and scalable, resistant ecosystems of enterprise applications.

3.1 Legacy Enterprise Systems Layer

The current enterprise applications provide the beginning of the modernization process which is typically implemented on the basis of traditional monolithic software architecture. These legacy systems have a wide scope and include most business processes including Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Supply Chain Management(SCM), Human Resource Management (HRM) and financial management, health care information systems, inventory management and e-commerce applications. Regardless of their track records of success in serving organizations over the years, these applications are generally correlated with a limited set of components, centralized databases, longer durations of deployment, lack of scalability and high maintainability costs.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

These old systems are expected to be examined and the initial step of the offered framework is to take into account the prospects of the modernization. The application level analysis is performed in depth as dependency analysis, business procedure analysis, data analysis evaluation and database software design analysis. The code analysis, which becomes AI enhanced, code modules reusability, dispensability and closely linked dependency and migratory priorities are all supplements of the AI-enhanced analysis. The astute review will help the organizations not only to craft an effective migration strategy, but to reduce business risks, as well as, provide business continuity throughout the modernization process.

3.2 Intelligent Service Decomposition Layer

The framework uses intelligent break down of systems within monolithic systems into deployable micro services which are independent of each other based on analysis of the legacy applications. Each is packaged within the microservices, which encapsulate an operational capability of a business entity and communicate with others all using standardized RESTful interfaces or gRPC interfaces. The domain-driven design principles are utilized to perform the decomposition and offer an excellent separation of responsibilities and minimal inter-service consulting.

The layer did entail different key activities such as domain-driven service; business capability mapping; API specification; service registry; centralized configuration; event modeling and database decomposition. Artificial intelligence is also needed since it is also used to examine software dependencies, behaviors of execution, and frequency of transactions; communications pattern between application modules. Based on such analyses, machine learning algorithms propose the optimum boundaries of services that would optimally achieve modularity and minimum communication overheads and service bondage.

Microservices that usually get generated are the User Management Service, Authentication Service, Product Service, Order processing Service, payment Service, notification Service, Inventory Service, Analytics Service, and Reporting Service. Their footloose characteristics mean that the entities are suitably maintainable, self-sufficient to deploy, discerningly expandable and simplified sustainment and quicker software development.

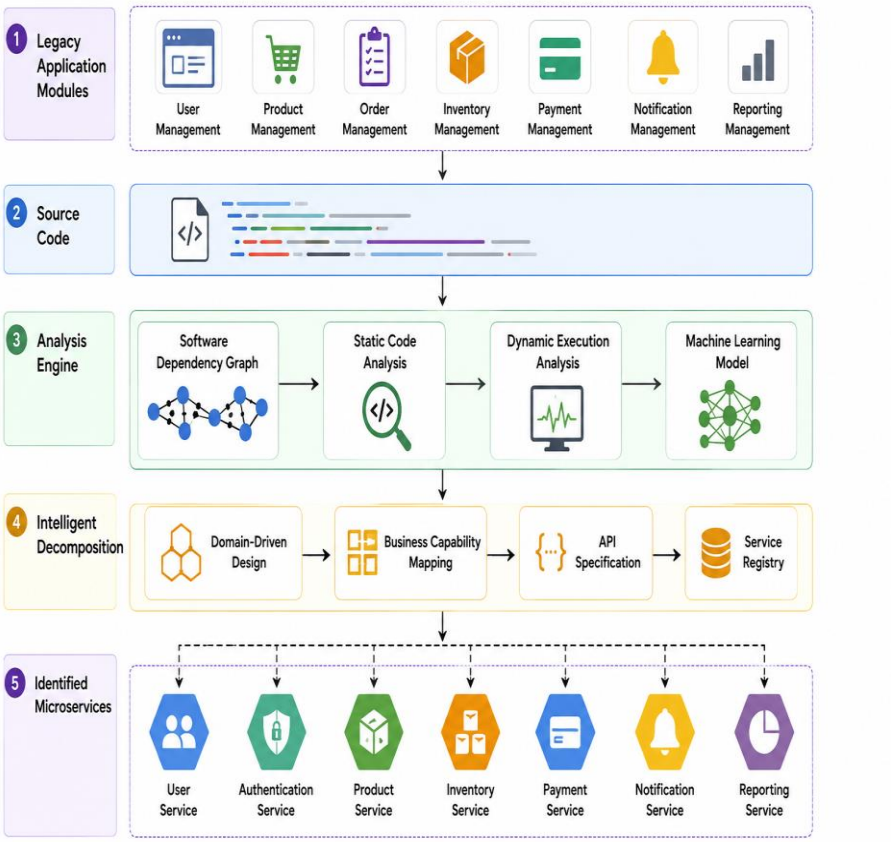

Figure 2- AI-Based Intelligent Service Decomposition Framework

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|
DOI: 10.15662/IJSRAT.2023.0602002

3.3 Cloud-Native Deployment Layer

The microservices are then coded into Docker containers and sent to the Google Kubernetes Engine (GKE) a fully managed Kubernetes engine owned and operated by Google. Containerization packages an app with its runtime environment and dependencies it needs, and asserts that it will be executable in the same environment in both development, testing and production. Kubernetes has workedload scheduling, self-healing, load balancing, horizontal pod autoscaling, service discovery and rolling updates as part of its offering of automated container orchestration.

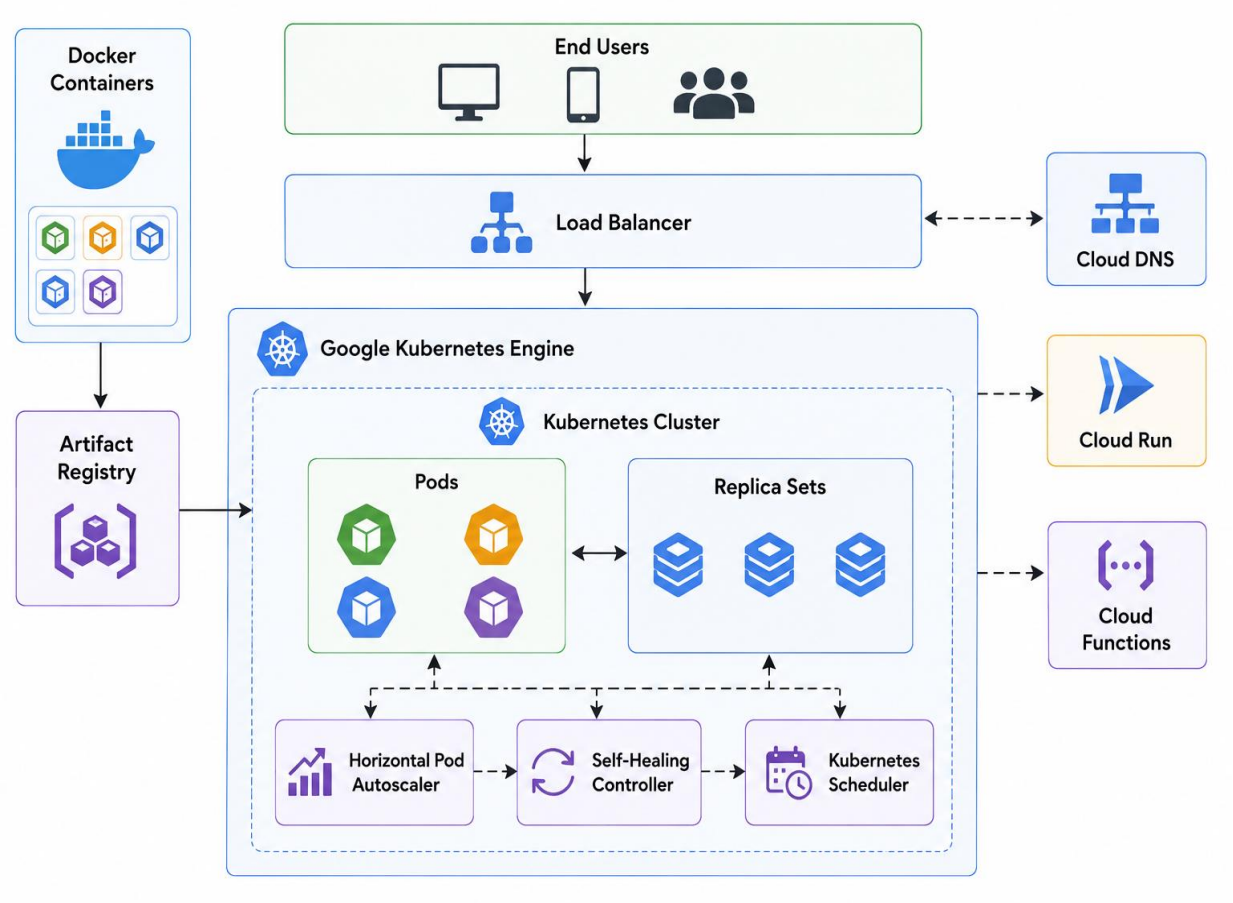

Figure 3- Cloud-Native Deployment and Orchestration Framework

The application tier incorporates a few controlling Google Cloud features, such as Google Kubernetes Engine (GKE), Cloud Run, Cloud Functions, Artifact Registry, Cloud Load Balancing, and Cloud DNS. Cloud Run is a tool used to run stateless microservices where the serverless invocation of the container would be more cost-effective to operate, and event-based workloads are reacted to with the help of Cloud Functions to constrain overheads of the underlying infrastructural management.

The orchestration features of Kubernetes monitor the health of applications, automatically restarts failed containers, balances workloads as the infrastructure has failed and undertakes the rolling upgrades without impacting the running of the business. The capabilities are very effective in enhancing the availability of applications, scalability and reliability of operation.

3.4 Event-Driven Communication Layer

The modern business systems require the loosely coupled communications mechanisms to be able to support asynchronous business processes, and the capability of responding to real time events. The proposed framework will employ event-based communication model where independent services will be able to communicate without heavy dependencies.

International Journal of Science, Research and Technology (IJSRAT)
|Bimonthly | Peer-Reviewed | Scholarly Journal|
|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|
DOI: 10.15662/IJSRAT.2023.0602002

This layer is a combination of Google Pub/Sub, Event Bus, API Gateway and Message queues and REST APIs and gRPC communication protocols. Asynchronous messages include business events like customer registration, payment confirmation, inventory, and shipments, fraud, and order completion and are published with Pub/Sub and handled independently by many microservices.

Event-driven model of communication has several advantages: It has fewer service coupling, increased scalabilities, fault tolerance, concurrent processing and enhanced system responsiveness. The API Gateway can also feature a centralized authentication, request routing, rate limiting, API authentication and monitoring the traffic in a way that will ensure that communications between the external customers and the internal Enterprise services will be safe and trustworthy.

3.5 Intelligent Data Management Layer

Another type of data produced by enterprise applications in the form of bulk data is structured, semi-structured and un structured data that must be stored, processed and analysed. The Intelligent Data Management Layer combines several Google Cloud based storage solutions to scale all types of enterprise workloads with high availability, high scalability and high performance.

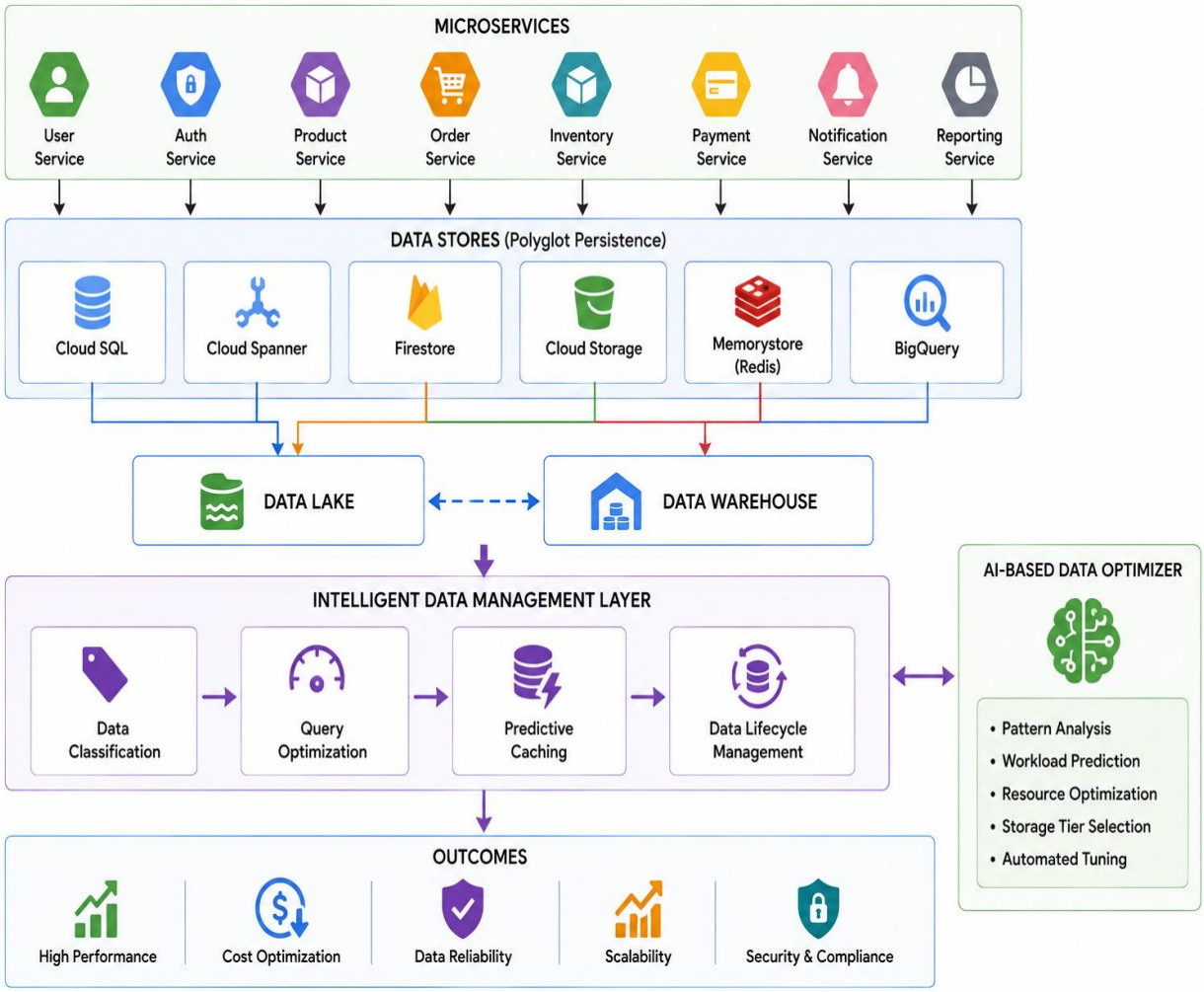

Figure 4- Intelligent Data Management Framework

The architecture proposed uses Cloud SQL, Cloud Spanner, Firestore, BigQuery, Cloud Storage and Memorystore (Redis). Micro services have their own database therefore eliminating the tight database couples and making the systems scalable. This decentralized data management also enables isolating fault as well as easy maintenance of databases.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

Artificial intelligence enhances the data management since it facilitates the data classification which is automated, intelligent searching of data, optimization of queries, predictive caching, selection of storage tier and data lifecycle. BigQuery is an analytical processor which can process huge amount of data at the enterprise level and Firestore offers the Latency and document-oriented, low-store which can be utilized to build business applications. All these services help not only in handling of the transactions, but also in the quality analytic services within the enterprise ecosystem.

3.6 AI-Driven Intelligence Layer

The main decision-maker of the proposed framework is artificial intelligence. The AI layer is the opposite of the traditional enterprise systems, which largely operate in accordance with the set rules, the AI layer constantly analyzes the metrics of operation, business actions, monitoring in the infrastructure, and interaction between people to simplify the enterprise.

Vernices AI Vertex AI, Tensorflow, AutoML, Machine Learning Pipelines, feature store and prediction APIs are used in the framework to develop, scale and sustain intelligent models. These models facilitate in predictive scaling, forecasting demand, intelligent scheduling of workloads, prediction of customer behavior, fraud detection, predictive failure in infrastructure, and efficient utilization of resources and formulation of recommendations, as well as long term capacity planning.

Continuously data are currently being gathered by historical, monitoring, transaction, and infrastructure telemetry to re-train the machine learning models, and are also improving predictions over time. AI also helps in Kubernetes scheduling whereby AI recommends the optimal location of workloads based on the CPU and memory utilization, network bandwidth, and latency requirements and priorities of the applications. This means that as the operational intelligence is continuously changing, so does the enterprise applications to some extent, assuming that it becomes more autonomous and adaptive.

3.7 Security and Governance Layer

As the applications of enterprises are increasingly spread, securing and governing is getting enormously more difficult. The proposed architecture includes comprehensive protection of cloud security that protects applications, services, data and infrastructure towards the path of the modernization lifecycle.

Identity and Access Management (IAM), Secret Manager, Cloud Armor, Web Application Firewall (WAF), OAuth 2.0, JWT Authentication, TLS encryption, Binary Authorization, Security Command Center and Virtual Private Cloud (VPC) Firewall Rules provide security. The outside requests are authenticated by all the microservices using secure identity tokens and all the microservices carry out the business operations; this is in order to ensure control of access to the distributed environment.

The framework embraces the principles of Zero Trust security by continually authenticating user identity, device trust, service identity, network context and API authorization by denying resources access. Proactive, real-time AI, scans the system operations to detect and report anomalous behavior: unusual login behavior, unauthorized access to the API, privileges-escalation behavior, abnormal network traffic, and suspicious service communications. Besides, it can minimize the risks of the software supply chain, as the constant scanning of images of the containers helps in increasing the cybersecurity of the enterprise.

3.8 Intelligent DevOps and Observability Layer

Constant software development has been a major requirement in today enterprise application. Computerized software development, infrastructure proving, deployment and management of monitoring and operation are performed as Intelligent DevOps and Observability Layer is aimed to promote a high quality of software and efficiency of its deployment.

The architectures combine Cloud Build, Cloud Deploy, Cloud Source Repositories, Artifact Registry, Terraform and Kubernetes Operators to create completely automated Devops pipelines. The Infrastructure as Code (IaC) enables declarative configuration files to be used to deploy compute and networking and storage, security policies, and cloud infrastructure.

Continuous integration and Continuous Deployment (CI/CD) pipelines automatically compile source code, do unit testing, scan security tests, do integration testing, create container images, deploy, rollback and manage versions. The Cloud Monitoring, Cloud Logging, Cloud Trace, Cloud Profiler, Error Reporting, and Alerting Policies are useful in

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

providing operational visibility. AI is also following through on the logs of the operations, the trace and the performance metrics continuously to detect the loss in performance before the users report a performance delay. Forecasting infrastructure failures: Predictive maintenance algorithms predict failures, recommend corrective controls and automatically inject self-healing workflows with Kubernetes Operators, significantly improving reliability and operational efficiency of enterprise applications.

Framework Workflow

The Intelligent Microservices Modernization Framework proposed above has a logical process task, where in the initial step, analysis of the existing enterprise applications is carried out to identify the business area, software dependencies and blockpoints of the architecture and location of the areas of exploitation to be given the first priority during the process of migration. Together with AI, service decomposition can be used to disaggregate monolithic applications into business-capability- Independent, deployable microservices. These are then moved to Google Kubernetes Engine, Cloud Run or Cloud functions in order to deploy them as containers.

The distributed services interact with one another via API Gateway and Google Pub/Sub that offers a chance to enable one with the other to relate to each other in a synchronous manner through API as well as asynchronously transferring and processing events. They are all distributed databases, cloud storage and BigQuery to enhance transactional processes, operations data management and scale analytics. Vertex AI is a continuous model that evaluates operational data to determine how to position the workloads, predict failures, identify anomalies, make predictions of resources and generate clever business insights. In the meantime, the principles of authentication and encryption, authorization, and ongoing monitoring and detection of the threat are realized through the Zero Trust security systems to the entire infrastructure. Lastly, automated DevOps pipelines control software development, testing, deployment, monitoring and provisioning infrastructure whilst observability services constantly check application performance, and start self-healing processes as necessary.

Benefits of the Proposed Framework

The Intelligent Microservices Modernization Framework proposed would help the enterprise modernization project in numerous aspects. The architecture can be scaled to high-levels with microservices that are independently available services that can be scaled independently based on the workload requirements. Kafka isolation and self-healing could also help in enhancing the resilience of applications and limiting disruptions in services to a minimum. Automated DevOps pipelines should be used to achieve quicker software development using continuous integration and deployment of software with minimum human efforts. The AI operational intelligence is used in predictive analytics, intelligent resource optimization, scheduling of workloads, anomaly identification and business decision-making.

The architecture also makes the enterprise more secure due to the help of the Zero Trust architecture, persistence checking, threat identification, driven by AI, and holistic access control. Serverless computing would allow them to optimize their costs by predictive autoscaling and efficient utilization of every node in the Google Cloud. Cloud services give ease to the management of the infrastructure and minimize the complexity of operating their businesses. It can be used to leverage business intelligence and advanced analytics using Vertex AI and BigQuery in real-time and interoperability of enterprise systems can be improved using standardized APIs and event-driven communication. Finally, automated backup, disaster recovery and self repair systems improve business continuity and ensure that business critical applications that are important to the business run efficiently.

The Intelligent Microservices Modernization Framework proposed in general can be taken as a step-by-step procedure to redesign the already existing enterprise application on Google Cloud Platform to an intelligent and cloud-native application. The framework will make the companies more agile, operational and resilient and will provide more agility and long-term sustainability by integrating microservice architecture, artificial intelligence, orchestration (Kubernetes), serverless computing, similar DevOps automation and intelligent insights into a single ecosystem, highly-dynamical-digital-environment.

IV. FRAMEWORK EVALUATION

To assess the performance of the suggested Intelligent Microservices Modernization Framework (IMMF), a comprehensive review was done based on the grounds of architactical traits, cloud-native functionalities, operation-intelligence, and scalability, security, and deployment efficiency. The assessment is aimed at understanding the effectiveness of the framework in tackling the drawbacks of traditional monolithic enterprise systems and with the assistance of Google Cloud Platform services, how to arrange intelligent enterprise modernization. The evaluation will

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

be designed into a mix of evaluation components that will include a general sense of viability and effectiveness of the suggested framework.

4.1 Scalability and Performance Evaluation

The suggested structure also goes a long way in enhancing the scalability of application as it breaks down monolithic application into deployable micro services. Each of the microservices can be horizontally scaled according to the load of the service with no impacts to the other service. Google Kubernetes Engine (GKE) has automatic method of orchestrating containers and scale up of horizontal pods and Cloud Run autoscaling of computing resources based on the incoming traffic. This architecture enables the utilization of cloud resources successfully and less over-providing of infrastructure. Communication based on event triggered processes with the help of Google Pub/Sub will also make the most out of the throughput in the sense that multiple business transactions can be executed asynchronously. The net effect is that the structure is most scaled and resistant to changes in loads on the enterprise.

4.2 Operational Intelligence Evaluation

Among the unique characteristics of the proposed framework, it is necessary to note that it implies integrating the artificial intelligence into the system of the operation management. Vertex AI processes infrastructure telemetry and application logs, history of transactions, and real-time monitoring metrics and projects foreseeable data. Smart models aid workload and demand modeling, prediction, anomaly modeling, prediction of scaling and infrastructure failure prediction. Compared to the conventional monitoring systems where the major response is created once the failure has occurred and the major response has already been made, the proposed system will enable the implementation of the decisions before the service interruption has taken place by identifying the potential worsening of the performance before the event actually takes place. This intelligent working ability increases the reliability and usability of resources of a venture significantly.

4.3 Security and Reliability Evaluation

To protect the distributed enterprise applications, the architecture has various security measures. The building blocks of the requisite pillars to create a safe cloud-native setup include Identity and Access Management (IAM), OAuth 2.0, JWT authentication, Cloud Armor, Binary Authorization, Secret Manager and TLS encryption. The implementation of the concepts of Zero Trust aims to realize the verification of a user and his/her identity, identity of the service and identity of network device, and situation in the network in near-real time before authorizing access to enterprise resources. To enhance availability of applications, Kubernetes self-healing capabilities will restart dying containers automatically, and will automatically reassign load in the event of the infrastructure failing. Examples of AI-enhanced cybersecurity include anomaly detection to monitor suspicious API requests, suspicious user activity, and unapproached transactions with services and are done in real-time.

4.4 Deployment Automation and DevOps Evaluation

The framework underlines the idea of continuous software delivery using fully automated DevOps pipelines. Cloud Build, Cloud Deploy, Terraform, Artifact Registry, and Kubernetes Operators are automation of compiling software, testing software, creating and testing container images, security test, deploying, rolling back and provisioning infrastructure. Passing infrastructure as Code means that there is minimal configuration error given that there is a consistent deployment both in development and production environments. CI/CD pipelines are also automated thus clocking less time on the deployment, better quality of the software and less time to deliver features. Cloud Dev.io Examples of tools of observability include Cloud Monitoring, Cloud Logging, Cloud Trace and Error Reporting that are built to give the entire picture of how an application behaves and its health.

4.5 Comparative Evaluation

The Intelligent Microservices Modernization Framework that is put forth to substitute the old-fashioned enterprise structures has immense advantages in various aspects. Monolithic systems can be defined as having no scalability, centralised deployment, sluggish releases and complex maintenance. The suggested framework, in turn, allows self-service implementation, smart workload balancing, infrastructure autoscaling, smart monitoring (AI) functionality, and strong cloud native operations. Kubernetes orchestration, no-code computing, AI-driven analytics, and DevOps automation are combined and integrated synergistically to create a very flexible business platform that can swiftly adapt to changes in business requirements. The framework hence provides a modernized, scaled and new method to modernization to be applied in organisations looking to transform the legacy enterprise applications into an agile, safe, and cloud-native infrastructure themed on Google cloud platform.

International Journal of Science, Research and Technology (IJSRAT)

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

V. CONCLUSION AND FUTURE WORK

Modernising enterprise applications has emerged as a tactical requirement of such organisations in a bid to gain more agility, scalability and robustness and higher operational efficiency in an ever competitive digital arena. Conventional monolith systems are frequently characterized by low scalability, slow deployment timelines, complicated maintenance, lack of support of newer technologies like artificial intelligence and cloud-native computing. The present paper has described the Intelligent Microservices Modernization Framework (IMMF) which utilizes Google Cloud Platform (GCP) to solve these issues by implementing cloud-native microservices, container orchestration, serverless computing, AI-based analytics, DevOps automation, intelligent monitoring, and end to end security across a single enterprise architecture. The suggested architecture takes advantage of Google Kubernetes Engine, Cloud Run, Cloud Functions, Google Pub/Sub, Vertex AI, BigQuery, Cloud SQL, Cloud Monitoring and Identity and Access Management to develop a highly resilient, secure, and scalable enterprise application ecosystem. The framework improves the scalability of the applications, nimble deployment of applications, fault tolerance, resource utilization and business continuity and minimizes the complexity of both infrastructure and the cost of intrinsic operation by decomposing existing monolithic applications into deployable microservices and autonomously manages the operations. This analysis reveals that with the help of artificial intelligence and cloud-native technologies, it is possible to operate resources upfront, automatically recover faults, proactively monitor and make more informed decisions, which contributes to the overall performance of the enterprise. Consequently, the proposed IMMF serves as a comprehensive roadmap to the organizations, which want to fast-track their digital transformation with intelligent cloud-native modernization on Google cloud platform.

The next study will be devoted to further evolution of the suggested framework by adding AIOps, Generative AI-based autonomous software agents, Large Language Models (LLMs) to solve intelligent applications and make self-adaptive decisions. The framework can also be extended to have multi-cloud interoperability with Google Cloud, Microsoft Azure, as well as the Amazon Web Services to provide workload portability and improved disaster recovery. Moreover, the research will focus on the exploration of the Green Cloud Computing, integration of Green Cloud Ballots with the edges and clouds, confidential computing, federated machine learning and AI based cyber security to enhance sustainability, security, compliance, and operational intelligence of the new generation enterprise systems. An experimental implementation in real life with real workloads of the enterprise and quantitative benchmarking of the framework will further prove the utility and load performance.

REFERENCES

[1] S. R. Goniwada, *Cloud Native Architecture and Design: A Handbook for Modern Day Architecture and Design with Enterprise-Grade Examples*. New York, NY, USA: Apress, 2022.
[2] A. Balalaie, A. Heydarnoori, and P. Jamshidi, “Microservices architecture enables DevOps: Migration to a cloud-native architecture,” *IEEE Software*, vol. 33, no. 3, pp. 42–52, May–Jun. 2016.
[3] N. Kratzke and P. C. Quint, “Understanding cloud-native applications after 10 years of cloud computing—A systematic mapping study,” *Journal of Systems and Software*, vol. 126, pp. 1–16, Apr. 2017.
[4] N. Kratzke and R. Peinl, “ClouNS—A cloud-native application reference model for enterprise architects,” in *Proc. IEEE 20th Int. Enterprise Distributed Object Computing Workshop (EDOCW)*, Vienna, Austria, 2016, pp. 1–10.
[5] C. Pahl, P. Jamshidi, and O. Zimmermann, “Architectural principles for cloud software,” *ACM Transactions on Internet Technology*, vol. 18, no. 2, pp. 1–23, 2018.
[6] C. Pahl and P. Jamshidi, “Microservices: A systematic mapping study,” in *Proc. 6th Int. Conf. Cloud Computing and Services Science (CLOSER)*, Rome, Italy, 2016, pp. 137–146.
[7] K. Bakshi, “Microservices-based software architecture and approaches,” in *Proc. IEEE Aerospace Conference*, Big Sky, MT, USA, 2017, pp. 1–8.
[8] J. Dobies and J. Wood, *Kubernetes Operators: Automating the Container Orchestration Platform*. Sebastopol, CA, USA: O’Reilly Media, 2020.
[9] Y. Brikman, *Terraform: Up & Running: Writing Infrastructure as Code*, 2nd ed. Sebastopol, CA, USA: O’Reilly Media, 2019.
[10] E. Bisong, “Kubeflow and Kubeflow Pipelines,” in *Building Machine Learning and Deep Learning Models on Google Cloud Platform*. New York, NY, USA: Apress, 2019, pp. 671–685.
[11] F. Y. Chemashkin and P. D. Drobintsev, “Kubernetes operators as a control system for cloud-native applications,” Tech. Rep., Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia, 2021.
[12] M. Szalay, P. Mátray, and L. Toka, “State management for cloud-native applications,” *Electronics*, vol. 10, no. 4, Art. no. 423, 2021.

|Bimonthly | Peer-Reviewed | Scholarly Journal|

|ISSN 2454-3853|www.ijsrat.com|editor@ijsrat.com|Vol.6, Issue 2, March-April 2023|

DOI: 10.15662/IJSRAT.2023.0602002

[13] S. Hendrickson, S. Sturdevant, T. Harter, V. Venkataramani, A. C. Arpaci-Dusseau, and R. H. Arpaci-Dusseau, "Serverless computation with OpenLambda," in *Proc. 8th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud)*, Denver, CO, USA, 2016, pp. 1–7.

[14] C. Moreno, R. A. C. González, and E. H. Viedma, "Data and artificial intelligence strategy: A conceptual enterprise big data cloud architecture to enable market-oriented organisations," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 6, pp. 7–14, 2019.

[15] H. Dinh-Tuan, F. Beierle, and S. Rodriguez Garzon, "Maia: A microservices-based architecture for industrial data analytics," in *Proc. IEEE Int. Conf. Industrial Cyber Physical Systems (ICPS)*, Taipei, Taiwan, 2019, pp. 23–30.