AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 1(2)(2026)

Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems

Santthosh Saai Reddy Purmani
RSA Tech Group LLC

Abstract: This research discusses the application of cloud-native AI architectures to change enterprise IT ecosystems. It discusses such important elements as data lakes, MLOps, RAG pipelines, agentic AI, and security layers with attention to scalability, flexibility, and security. With the help of industry case studies and scholarly literature, the paper identifies the industry best practices of cloud-native AI implementation and outlines some of the challenges encountered by CIOs in ensuring business alignment. It also highlights the fact that long-term architectural planning is necessary to enable AI systems to be future-proof so that they can be scaled and modified to meet future changes in technology.

Keywords: Cloud-native AI, Scalability, MLOps, Data Lakes, RAG Pipelines, Agentic AI, Security Layers, Long-term Planning

I.INTRODUCTION

Cloud-native AI architecture combines artificial intelligence with a scalable cloud architecture that is flexible, scalable, and secure. Cloud-native systems must be designed to process the growing use of AI technologies by organizations, the large volumes of data, and to integrate it smoothly. There is an increased need to have scalable, secure, and intelligent IT ecosystems, especially in businesses that are more concerned with innovation and data-driven decision-making.

Problem Statement

Organizations face significant challenges in implementing cloud-native AI architectures that are scalable, secure, and aligned with business objectives.

The problem statement points out the challenge that organizations experience in embracing cloud-native AI designs. These architectures can be scalable, secure, and business-aligned. Making these components work together in many companies is a challenge, as businesses are facing difficulties trying to strike a balance between scalability, security, and business goals, and achieving the maximum performance of AI.

Aim and Objectives

Research Aim

To explore the design, scalability, security, and intelligence of cloud-native AI architectures in enterprises.

Objectives

1. To evaluate the role of cloud-native AI architecture in supporting scalable, secure, and intelligent IT ecosystems.
2. To explore the integration of data lakes and MLOps in cloud-native AI systems for seamless deployment.
3. To identify challenges faced by CIOs in adopting cloud-native AI architectures across different industries.
4. To recommend best practices for implementing cloud-native AI architectures that align with organizational goals.

Research Rationale

As enterprises embrace AI technologies, there is a growing need to have scalable, secure, and efficient architectures. AI technologies are important to understand how cloud-native AI can be used to meet these needs in order to have future-proof IT systems [1]. The reason behind this research is that it can fill the gap in the literature, as it can present practical information on how to create AI-first infrastructures to make businesses successful.

Significance of the Study

The paper is valuable to any enterprise that is interested in implementing AI technologies on top of scalable and secure cloud-native systems. The secure cloud-native system has been able to equip the CIOs with the necessary knowledge in making sound decisions regarding IT system design, security, and long-term strategic plans [2]. This study can be relevant to the best practices in AI architecture.

II. LITERATURE REVIEW

Evaluating Cloud-Native AI Architecture's Role in Scalability and Security

The assessment of cloud-based artificial intelligence architecture regarding scalability and security is of importance to contemporary organizations. Cloud native systems are created to take advantage of the flexibility and scalability of cloud computing and thus are designed well to manage large-scale workloads of AI [3]. These architectures allow organizations the ability to scale their AI applications in a smooth way through the use of cloud services such as elastic computing resources, on-demand storage, and a distributed network. The scalability is necessary because of the companies that operate with a lot of information and need to process it in real-time.

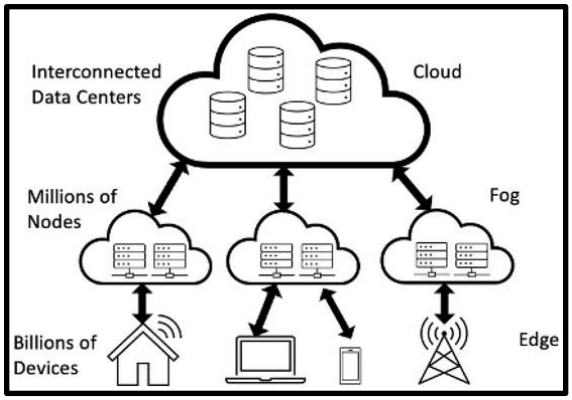

Fig 1: AI and Computing Horizons: Cloud and Edge in the Modern Era

Scalability is not enough. Security is a primary issue when it comes to the integration of AI in the cloud-native environment. The AI systems handle sensitive data, exposing them to cyber threats, such as data breaches and adversarial attacks [4]. Cloud-native AI systems should include advanced security precautions that secure these systems. Cloud-native AI involves encrypting data, using secure access controls, multi-factor authentication, and screening AI models on a regular basis [5]. Organizations can reduce risks by incorporating security layers into the structure to guarantee that their AI systems do not violate privacy laws. Security can also be evaluated in the sense of how the AI architecture of cloud-native can be implemented without affecting scalability [6]. A balance between these two aspects ensures that companies can expand their AI without data loss and maintain their privacy and confidentiality. Finally, AI architecture is cloud-native, and it is important in providing scalable and safe solutions to enterprise applications.

Exploring Integration of Data Lakes and MLOps in Cloud-Native AI

Cloud-native AI solutions rely on the combination of data lakes and MLOps. Data lakes enable organizations to store large volumes of unstructured and structured data that is available to train AI models and analyze [7]. As the amount of data within enterprises increases, data lakes are used as a centralized place to store large datasets within them, allowing them to be stored and accessed easily. Such integration can provide the AI models with the data that they need to learn and develop. MLOps simplifies the machine learning models deployment, monitoring, and management process in the production environment [8]. MLOps is associated with the continuous integration and deployment process; hence, through automation of these processes, companies can respond to shifting business demands rapidly.

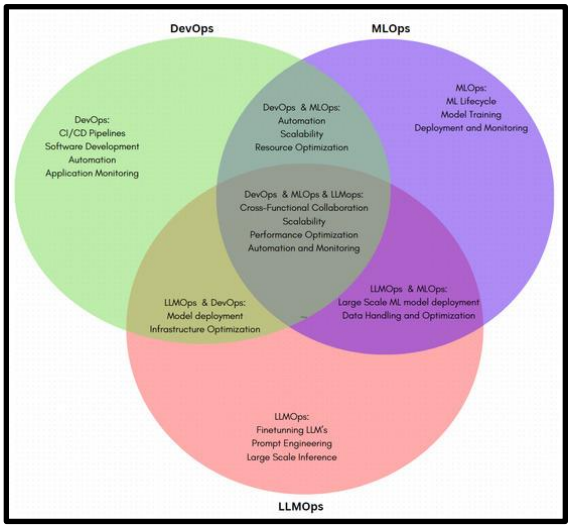

Fig 2: Transitioning from MLOps to LLMOps

The union of data lakes and MLOps makes AI applications in the cloud-native environment efficient and scalable. Data lakes facilitate data quality and governance that are critical in the proper modeling of AI, whereas MLOps keep the models alive and current [9]. MLOps also helps to integrate data scientists and the operations team and eliminate the disconnect between model development and deployment. With this type of integration, organizations have a better way of managing their AI lifecycle, including the ingestion of data as well as the deployment of models. The AI lifecycle makes cloud-native AI architectures less efficient, agile, and responsive to the needs of the organization [10]. This data lake and MLOps integration is a seamless process that is needed to implement the success of AI-powered solutions.

Identifying Challenges for CIOs in Adopting Cloud-Native AI Systems

The challenges of adopting cloud-native AI systems among the enterprises by the CIOs include a number of challenges. The significant issue is the ability to integrate with the current infrastructure without difficulties [11]. There are many organizations that have legacy systems, and it is hard to switch to a cloud-native environment. Migration to cloud native architecture involves a major IT infrastructure change that can prove expensive and time-consuming [12]. Moreover, CIOs should ensure that their staff possesses the skills required to use and maintain cloud-native AI systems. It is not always easy to upskill teams and acquire talent to work with cloud-native environments, particularly in industries where qualified specialists are scarce.

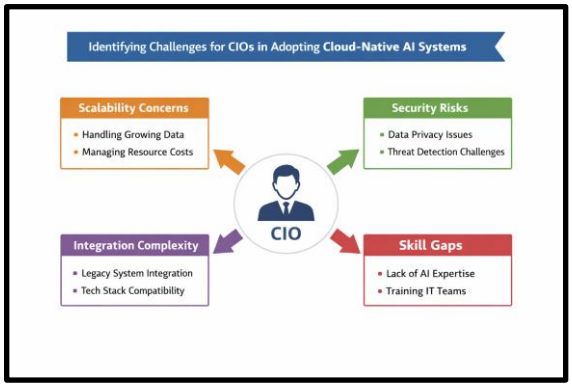

Fig 3: CIO challenges in adopting AI systems

The other issue is the security and compliance of data. AI systems can deal with sensitive information, and cloud-native environments raise the vulnerability to cyber threats [13]. The CIOs should make sure that they have strong security controls that can safeguard data and make sure that they meet the regulations, such as GDPR or HIPAA. The security and scalability of cloud-native systems need to be adequately planned [14]. Moreover, AI models should be monitored in terms of performance and accuracy continuously. CIOs have to cope with the difficulty of model integrity, model drift, and guarantee the reliability of AI model results and their unbiasedness [15]. The complexity of using AI-managed systems is a cloud-native architecture issue that needs strategic leadership and vision.

Recommending Best Practices for Implementing Cloud-Native AI Architectures

Recommending best practices for implementing cloud-native AI architectures is essential to ensuring long-term success and scalability. The organizations can prioritize a robust and flexible cloud infrastructure that can easily scale with growing AI demands [16]. This includes adopting cloud services that offer elastic compute resources, on-demand storage, and flexible networking capabilities. By selecting the right cloud provider, businesses can ensure they have the resources needed for AI applications to run efficiently at scale. Adopting microservices and containerization allows AI workloads to be decoupled, promoting better resource management and faster deployment.

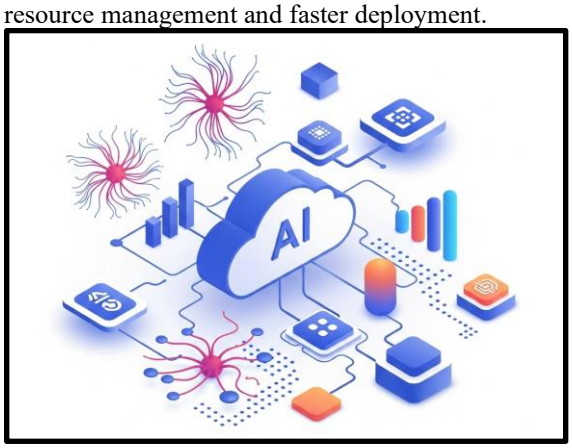

Fig 4: Cloud-Native AI Applications Development

Secondly, implementing data governance and quality control measures is critical to the success of AI models in cloud-native architectures. Organizations must establish clear data management policies that ensure the consistency, accuracy, and accessibility of data across all AI systems [17]. This includes setting up data lakes with structured and unstructured data, ensuring seamless integration with machine learning models. Organizations can adopt AI development MLOps practices, allowing for automated model deployment, continuous integration, and monitoring [18]. Lastly, security should be embedded at every level of the architecture. Implementing encryption, secure access control, and regular vulnerability assessments can safeguard AI systems and data from cyber threats. Organizations can build AI-first architectures that are scalable, secure, and future-proof by following these best practices.

Table 1: Best Practices for Implementing Cloud-Native AI Architectures

Best Practice	Description
Scalable Infrastructure	Prioritize flexible cloud services for scaling AI workloads efficiently.
Data Governance and Quality Control	Implement policies ensuring consistent, accurate, and accessible data.
MLOps Integration	Adopt continuous integration and deployment for automated model management.
Security Measures	Embed encryption, access controls, and regular assessments for AI system protection.

Literature Gap

Despite the growing adoption of cloud-native AI architectures, there is limited research addressing the integration of data lakes, MLOps, and security within these systems. Current studies often focus on isolated components of cloud-native AI or on specific industries [19]. There is a lack of comprehensive frameworks that combine scalability, security, and AI-driven intelligence. This literature gap highlights the need for a holistic approach that integrates cloud-native AI, data management, and operational practices while addressing the challenges faced by CIOs in diverse organizational contexts.

III. METHODOLOGY

The research design of Artificial Intelligence First Enterprise Architecture: The Design of Scalable,

Secure, and Intelligent IT Ecosystems is split into three primary phases that include data collection, design framework development, and tools and technologies research. The stages are designed to offer a comprehensive method for the design and implementation of AI-driven enterprise architecture.

Data Collection:

Case studies can be used to gather data on companies that have deployed AI-first enterprise architecture. The case studies will be used to shed light on the actual implementation of AI technologies in the real world in terms of scalability, security, and intelligent systems [20]. The information will be accessed through the interviews with enterprise architects, business analysts, and IT professionals. Also, openly accessible case studies and industry reports will be examined to learn about the difficulties and advantages of AI-first architecture.

Design Framework:

An IT architecture will be suggested to incorporate AI into enterprise architectures. This framework will prioritize three main elements: scalability, security, and intelligence. The structure of the framework will be the following:

Scalability: The AI will be built in such a way that it can be scaled vertically and horizontally with ease, as systems can manage more data and users.

Security: AI-based security will be integrated to protect the enterprise systems by detecting anomalies, predicting threats, and responding to incidents automatically.

Intelligence: AI will improve the decision-making process through predictive analytics, real-time insights, machine learning models, and routine task automation.

Tools and Technologies:

When working on the implementation of the AI-first enterprise architecture, one is going to consider several major technologies:

Machine Learning (ML): ML algorithms will streamline the work of the system and decision-making.

Cloud computing: Cloud computing will allow the scaling and adaptable implementation of AI models.

IoT: IoT-driven data collection and processing into real-time data will be applied, and AI will be able to provide actionable information.

Big Data Analytics: AI models will analyze large amounts of data that big data technologies will streamline and convert into trend and pattern revelations.

IV. RESULT AND DISCUSSION

Cloud-Native AI Architecture Design: Scalability, Flexibility, and Deployment

Cloud-native AI systems allow companies to achieve the scale of their systems through cloud services. These architectures make sure that organizations are able to process data volumes that are rapidly growing and to conduct sophisticated AI-driven operations without a hitch. Cloud-native AI systems are flexible due to the use of microservices and containerized applications, which can enable companies to launch AI models with low overhead [21]. Cloud-native systems have quicker deployment, reduced implementation, and are more highly available than conventional on-premise solutions.

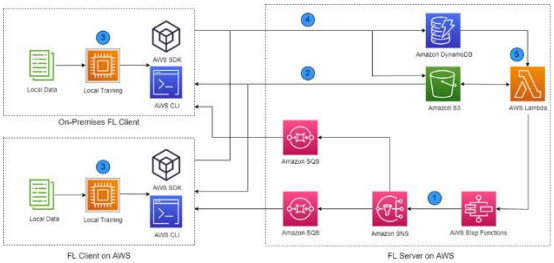

Fig 5. Cloud-Native AI Architecture Design: Scalability, Flexibility, and Deployment

Studies by major technology companies, including Netflix and Google, have indicated that cloud-native architectures save a lot of money used to manage infrastructure, besides being scalable. Kubernetes and containerization can also help organizations to scale and manage AI applications on demand as cloud-native AI systems [22]. An illustration of this is in the healthcare industry, where AI systems based on cloud-native architecture process medical imaging, patient data, and research datasets on a large scale in real-time.

Role of Data Lakes in AI Systems: Supporting Scalable Storage for AI Workloads

Data lakes are important in aiding AI workloads through the provision of scalable and flexible data storage. The amount of unstructured and structured data continues to grow; data lakes help an organization store and process large volumes of data needed to train AI models [23]. Data lakes, in contrast to traditional databases, enable businesses to feed and put raw data, and then clean and put it into an organized format that can be used in AI-based decision-making.

Table 2: pseudocode for Data Lakes in AI Systems

```
"BEGIN

  // Define the Data Lake structure
  DEFINE DataLake:
    - Scalable storage system for structured and unstructured data
    - Data hierarchy: Raw, Processed, Curated data

  // Establish connection to the Data Lake
  FUNCTION ConnectToDataLake():
    - Set access credentials (API keys, tokens)
    - Authenticate connection

  // Load data into the Data Lake
```

```
    FUNCTION
LoadDataToDataLake(data_source,
destination_path):
        - Retrieve data from the source (e.g., IoT
devices, databases)
        - Preprocess data (clean, filter)
        - Store the data in DataLake at
destination_path
        - Log success/failure

    // Retrieve data from Data Lake for AI
Workloads
    FUNCTION
RetrieveDataFromDataLake(query_parameters):
        - Query the DataLake with parameters (e.g.,
data type, time range)
        - Filter the data based on query criteria
        - Return filtered data for AI use

    // Process and transform data for AI Models
    FUNCTION PreprocessDataForAI(data):
        - Handle missing values (remove or impute)
        - Normalize or scale data
        - Extract features (e.g., image resizing, text
tokenization)
        - Return processed data

    // Example of loading and processing data
    data_source = "Sensor_Data"
    destination_path = "Raw/SensorData/"
    LoadDataToDataLake(data_source,
destination_path)

    query_parameters = {"data_type":
"temperature", "time_range": "last_30_days"}
    raw_data =
RetrieveDataFromDataLake(query_parameters)

    processed_data =
PreprocessDataForAI(raw_data)

    // Use processed data in an AI model for
training or inference
    model_output =
AI_Model.Train(processed_data)  // If training
    // OR
    model_output =
AI_Model.Predict(processed_data)  // If
inference

    RETURN model_output

END
"
```

Data lakes have been combined with AI systems in such industries as finance and retail to provide insights and decision-making procedures. To illustrate this, financial institutions store the information about transactions in data lakes and use machine learning algorithms to identify fraudulent behavior.

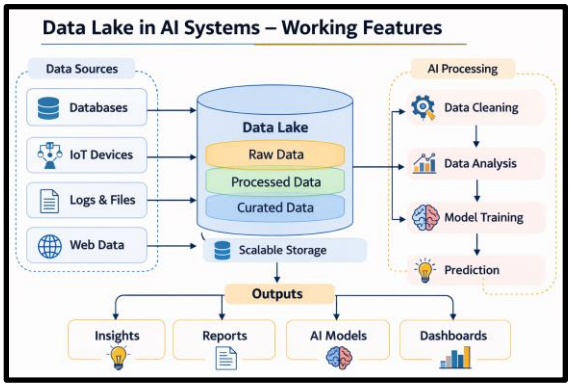

Fig 6. Data Lake in AI Systems – Working Features

Firms such as Amazon and Walmart use data lakes to advance their customer experience by improving their recommendation engines to boost sales. Traditional data storage systems are rather unfamiliar to the high-volume, real-time analytics that AI systems need, in comparison.

MLOps for AI Deployment: Optimizing Model Deployment, Monitoring, and Improvement

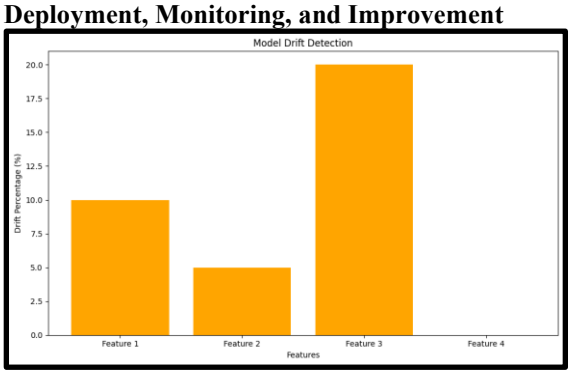

Fig 7. Model Drift Detection

MLOps (Machine Learning Operations) has turned into a critical practice in streamlining the deployment, monitoring, and perpetual enhancement of the machine learning models. MLOps are incorporated into cloud-native AI, and enterprises are able to automate the deployment of models, track their performance, and perform lifecycle operations [24]. MLOps can greatly boost the use of AI by reducing the overall workflow between the data science team and the production system in favor of faster model development.

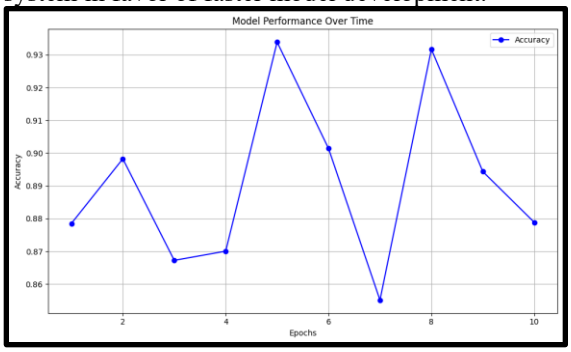

Fig 8. Model Performance Over Time

MLOps promotes more collaboration and uniformity in comparison to the traditional AI model deployment processes. AI model deployment processes allow continuous integration and continuous deployment (CI/CD) pipelines that help businesses deploy updated models in a very short time [25]. Microsoft and Uber employ MLOps practices to make sure that their AI systems are correct and functional, as new data is actively consumed. In addition, MLOps facilitates model governance where AI models are made in line with industry standards and regulations.

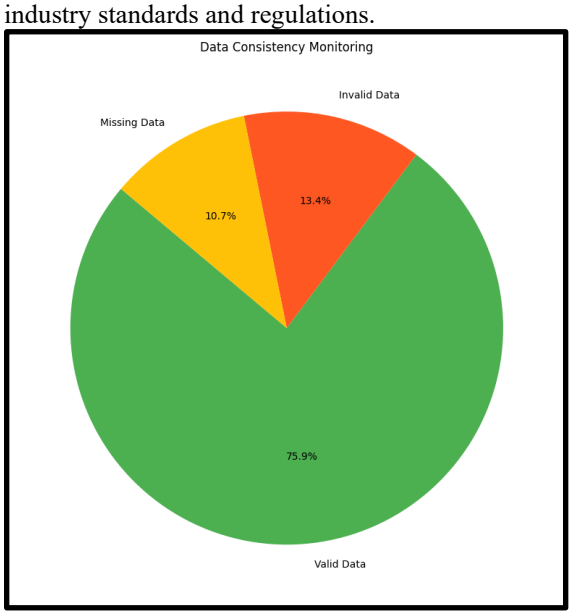

Fig 9. Data Consistency Monitoring

Security Layers in Cloud-Native AI: Protecting Models and Data from Cyber Threats

AI systems are not at risk; a combination of various security techniques is needed. The priority of implementation of cloud-native AI systems is security because AI models and data are susceptible to cyber threats, such as data leaks and adversarial assaults [26]. Security measures that are commonly provided by cloud-native AI architecture to protect data and models include encryption, access controls, secure APIs, and anomaly detection.

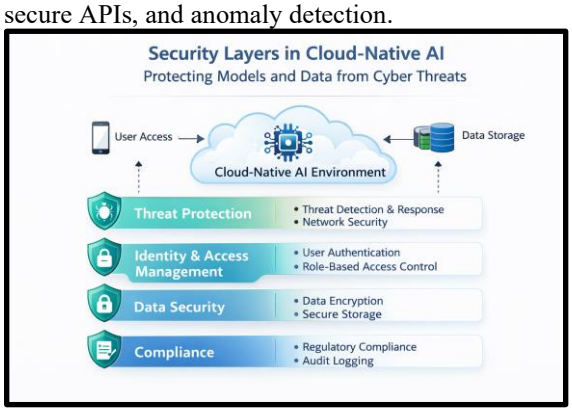

Fig 10. Security Layers in Cloud-Native AI

The security layers in cloud-native AI systems are easier to implement in the architecture than traditional systems. The containerization and microservices also allow an organization to segregate AI workloads that do not allow unauthorized access to sensitive data [27]. Firms such as Google and Amazon have strong security measures in place to make sure that applications that are run by AI do not violate data privacy laws, including etc. GDPR. Moreover, the AI-driven anomaly detection systems can improve the possibility of the system detecting security infractions before they occur.

Long-Term Architectural Planning from the CIO Perspective

CIOs need to make long-term architectural plans to achieve the success of cloud-native AI systems. The businesses that are larger in scale take their initial steps towards AI-first architectures, CIOs have to think about how to grow and scale, and how these systems can align with the business goals. Cloud-native AI architectures should be elastic to enable the use of emerging technologies and adapt to new business needs [28]. Also, a CIO should evaluate the ability of its systems to withstand possible changes in the future, as it is expected to store more data than is previously anticipated, and involve AI technologies.

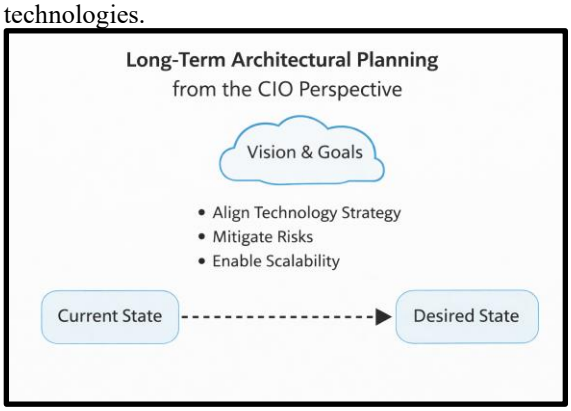

Fig 11. Long-Term Architectural Planning

Cloud-native solutions are becoming a popular trend among CIOs because of the flexibility that they offer in future development. The adoption of the microservices architecture can enable organizations to seamlessly implement new AI technologies without interfering with the existing systems [29]. In addition, data management and security policy are to align with long-term goals so that AI models can be kept in accordance with changing regulations. This is proactive planning that enables organizations to survive in the fast-evolving world of AI.

V. CONCLUSION

In conclusion, cloud-native AI-based systems are important in reshaping enterprise IT frameworks, providing them with scalability, flexibility, and increased deployment efficiency. Data lakes, MLOps, RAG pipelines, agentic AI, and a solid security layer can ensure the optimization of AI systems, their security, and continuous enhancement. With more companies implementing AI technologies, the need to emphasize long-term architectural planning by CIOs to balance between scalability and security is becoming more important.

With the best practices and the solution of cloud-native AI, enterprises can become more innovative, efficient in their operations, and competitive within a fast-changing technological environment.

Future Scope

The future of cloud-native AI architecture is the development of additional capabilities in the areas of scalability, security, and compatibility with new technologies. Quantum computing can be studied in combination with a cloud-native AI system that can provide unprecedented processing power. The increasing significance of federated learning opens the opportunities of decentralized AI models while preserving the privacy of the data [30]. The development of improved security frameworks should also serve as a future area of work to counter the ever-advanced cyber threats. In addition, the discussion of AI-based automation in MLOps can contribute to better model management. Continued study of AI in AI-first enterprises should also focus on long-term sustainability and ethical application of AI.

VI. REFERENCES

[1] Katsaros, K., Mavromatis, I., Antonakoglou, K., Ghosh, S., Kaleshi, D., Mahmoodi, T., Asgari, H., Karousos, A., Tavakkolnia, I., Safi, H. and Hass, H., 2024. AI-native multi-access future networks—The REASON architecture. *IEEE Access*, *12*, pp.178586-178622.

[2] Al-Marsy, A., Chaudhary, P. and Rodger, J.A., 2021. A model for examining challenges and opportunities in use of cloud computing for health information systems. *Applied System Innovation*, *4*(1), p.15.

[3] Parasaram, V.K.B., 2022. Converging Intelligence: A Comprehensive Review of AI and Machine Learning Integration Across Cloud-Native Architectures. *International Journal of Research & Technology*, *10*(2), pp.29-34.

[4] Adeyeye, O.J., Akanbi, I., Emeteveke, I. and Emehin, O., 2024. Leveraging secured AI-driven data analytics for cybersecurity: Safeguarding information and enhancing threat detection. *International Journal of Research and Publication and Reviews*, *5*(10), pp.3208-3223.

[5] SAMUEL, A., 2021. Cloud-Native AI solutions for predictive maintenance in the energy sector: A security perspective. *Available at SSRN 5290068*.

[6] Oladosu, S.A., Ige, A.B., Ike, C.C., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2022. Next-generation network security: Conceptualizing a unified, AI-powered security architecture for cloud-native and on-premise environments. *International Journal of Science and Technology Research Archive*, *3*(2), pp.270-280.

[7] Nambiar, A. and Mundra, D., 2022. An overview of data warehouse and data lake in modern enterprise data management. *Big data and cognitive computing*, *6*(4), p.132.

[8] Hanchuk, D.O. and Semerikov, S.O., 2024. Implementing MLOps practices for effective machine learning model deployment: A meta synthesis. In *AREdu* (pp. 329-337).

[9] Lakarasu, P., 2022. MLOps at Scale: Bridging cloud infrastructure and AI lifecycle management. *Available at SSRN 5272259*.

[10] Parasaram, V.K.B., 2022. Converging Intelligence: A Comprehensive Review of AI and Machine Learning Integration Across Cloud-Native Architectures. *International Journal of Research & Technology*, *10*(2), pp.29-34.

[11] Ugwueze, V.U., 2024. Cloud native application development: Best practices and challenges. *International Journal of Research Publication and Reviews*, *5*(12), pp.2399-2412.

[12] Al-Marsy, A., Chaudhary, P. and Rodger, J.A., 2021. A model for examining challenges and opportunities in use of cloud computing for health information systems. *Applied System Innovation*, *4*(1), p.15.

[13] Celeste, R. and Michael, S., 2021. Next-Gen Network Security: Harnessing AI, Zero Trust, and Cloud-Native Solutions to Combat Evolving Cyber Threats. *International Journal of Trend in Scientific Research and Development*, *5*(6), pp.2056-2069.

[14] Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., Girolamo, M.D. and Barone, P., 2023. Security in cloud-native services: A survey. *Journal of Cybersecurity and Privacy*, *3*(4), pp.758-793.

[15] Ledro, C., Nosella, A. and Dalla Pozza, I., 2023. Integration of AI in CRM: Challenges and guidelines. *Journal of Open Innovation: Technology, Market, and Complexity*, *9*(4), p.100151.

[16] Haefner, N., Parida, V., Gassmann, O. and Wincent, J., 2023. Implementing and scaling artificial intelligence: A review, framework, and research agenda. *Technological Forecasting and Social Change*, *197*, p.122878.

[17] Tadi, V., 2020. Optimizing data governance: Enhancing quality through AI-integrated master data management across industries. *North American Journal of Engineering Research*, *1*(3).

[18] Hanchuk, D.O. and Semerikov, S.O., 2024. Implementing MLOps practices for effective machine learning model deployment: A meta synthesis. In *AREdu* (pp. 329-337).

[19] Ugwueze, V.U., 2024. Cloud native application development: Best practices and challenges. *International Journal of Research Publication and Reviews*, *5*(12), pp.2399-2412.

[20] Sundaramurthy, S.K., Ravichandran, N., Inaganti, A.C. and Muppalaneni, R., 2022. AI-powered operational resilience: Building secure, scalable, and intelligent enterprises. *Artificial Intelligence and Machine Learning Review*, *3*(1), pp.1-10.

[21] Oyeniran, O.C., Modupe, O.T., Otitoola, A.A., Abiona, O.O., Adewusi, A.O. and Oladapo, O.J., 2024. A comprehensive review of leveraging cloud-native technologies for scalability and resilience in software development. *International Journal of Science and Research Archive*, *11*(2), pp.330-337.

[22] Ugwueze, V.U., 2024. Cloud native application development: Best practices and challenges. *International Journal of Research Publication and Reviews*, *5*(12), pp.2399-2412.

[23] Nambiar, A. and Mundra, D., 2022. An overview of data warehouse and data lake in modern enterprise data management. *Big data and cognitive computing*, *6*(4), p.132.

[24] Parasaram, V.K.B., 2022. Converging Intelligence: A Comprehensive Review of AI and Machine Learning Integration Across Cloud-Native Architectures. *International Journal of Research & Technology*, *10*(2), pp.29-34.

[25] Mohammed, A.S., Saddi, V.R., Gopal, S.K., Dhanasekaran, S. and Naruka, M.S., 2024, March. AI-Driven continuous integration and continuous deployment in software engineering. In *2024 2nd International Conference on Disruptive Technologies (ICDT)* (pp. 531-536). IEEE.

[26] Ofili, B.T., Obasuyi, O.T. and Osaruwenese, E., 2024. Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. *Int J Eng Technol Res Manag*, *8*(11), p.631.

[27] Kansara, M., 2021. Cloud migration strategies and challenges in highly regulated and data-intensive industries: A technical perspective. *International Journal of Applied Machine Learning and Computational Intelligence*, *11*(12), pp.78-121.

[28] Parasaram, V.K.B., 2022. Converging Intelligence: A Comprehensive Review of AI and Machine Learning Integration Across Cloud-Native Architectures. *International Journal of Research & Technology*, *10*(2), pp.29-34.

[29] Pandiya, D.K. and Charankar, N., 2023. Integration of microservices and AI for real-time data processing. *International journal of computer engineering and technology (IJCET)*, *14*(2), pp.240-254.

[30] Beltrán, E.T.M., Pérez, M.Q., Sánchez, P.M.S., Bernal, S.L., Bovet, G., Pérez, M.G., Pérez, G.M. and Celdrán, A.H., 2023. Decentralized federated learning: Fundamentals, state of the art, frameworks, trends, and challenges. *IEEE Communications Surveys & Tutorials*, *25*(4), pp.2983-3013.