Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

Cyber Threat's in Cloud Computing: Challenges and Solutions

Sahas Bochare
Undergraduate Student, Department of Information and Technology,
St. John College of Engineering and Management, Palghar, Maharashtra, India

Abstract **- This compilation of research papers provides a multifaceted overview of cloud computing, focusing on its evolving paradigms, inherent security challenges, and the role of advanced technologies in addressing them. Cloud computing is defined as a technology that delivers services to clients via the internet, allowing for the rental of required services through web browsers. It is characterized by pervasive features like online storage, high scalability, and seamless accessibility, which significantly reduce capital costs and workforce needs for organizations. This technology is closely related to big data, which focuses on extracting value from massive, heterogeneous datasets that are difficult to store and manage with traditional methods. A central theme across these papers is security, a critical concern that proportionally increases with cloud usage. Traditional security measures often struggle against sophisticated cyber threats in cloud environments. To bolster security, Deep Learning (DL) and Machine Learning (ML) techniques are highlighted as powerful tools for identifying and addressing cloud security threats. These include anomaly detection, security automation, cloud-native security, image-based detection, network traffic analysis, and the role of emerging technologies. Despite the growth in this research area, challenges such as data privacy, scalability, and explainability, along with integration issues and performance concerns, remain to be addressed. Overall, these papers collectively highlight that while cloud computing offers significant advantages, its effective and secure implementation necessitates continuous innovation in security measures, thoughtful development of new computing paradigms, and systematic approaches to migration and quality assurance, with ongoing research crucial for addressing evolving challenges and ensuring compliance with regulations.**

Keywords **- Cloud Computing, Security, Machine Learning (ML), Big Data, Serverless Computing, Cloud Migration.**

INTRODUCTION

The provided research papers collectively offer a comprehensive overview of the evolving landscape of cloud computing, addressing its foundational concepts, emerging paradigms, critical security challenges, and the role of advanced technologies in its development and maintenance [1]. Cloud computing is fundamentally defined as a technology that delivers services to clients over the internet, enabling them to rent necessary services via web browsers [2]. This paradigm is characterized by pervasive features such as online storage, high scalability, and seamless accessibility, which contribute significantly to reducing capital costs and workforce requirements for organizations [3]. Its close relationship with big data is highlighted, as big data—defined as datasets that are too large, heterogeneous, and complex to be stored, managed, and analyzed by traditional methods—requires efficient processing and storage solutions that cloud computing environments can provide [4]. A paramount and recurrent theme across these studies is security, whose importance increases proportionally with cloud usage. Traditional security measures are often inadequate against the sophisticated cyber threats prevalent in cloud environments, making robust security a critical concern [5]. To counter these escalating threats, Deep Learning (DL) and Machine Learning (ML) techniques are identified as powerful tools for enhancing cloud security. These techniques are applied to various security challenges including anomaly detection, security automation, cloud-native security, image-based malware detection, network traffic analysis, insider threat detection, and the integration of emerging technologies like blockchain and quantum-resistant cryptography [6]. Despite the significant growth in research leveraging ML and DL for cloud security since 2006 for ML and 2014 for DL, persistent challenges include data privacy, scalability, explainability, generalizability, label bias, integration issues, and performance concerns [7].

The papers also delve into various cloud computing paradigms and their strategic implications: Serverless Computing: This emerging field, also known as Function-as-a-Service (FaaS), has gained considerable importance for its ability to reduce costs, decrease latency, improve scalability, and eliminate server-side management. Surveys explore its fundamental concepts, platforms (such as AWS Lambda, Apache OpenWhisk, and Azure Functions), various use cases, and the challenges it faces, including the "cold start" problem, resource limits, and the lack of comprehensive debugging and monitoring tools. Future research is focused on overcoming these issues and facilitating the migration of legacy systems to serverless architectures.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

Cloud Migration: Relocating mission-oriented enterprise applications to the cloud is recognized as an important strategic IT task and it requires a rigorous process. Cloud migration approaches that currently exist are analyzed and evaluated, showing similarities, activities, guidance and methods. Key challenges in this domain include a lack of sound research quality in proposed methodologies, insufficient support for cloud-specific features like multi-tenancy and elasticity, and the absence of a unified process model for cloud migration. The importance of understanding legacy applications and their impact on migration is also emphasized.

Cloud-Native Computing: Described as the most influential development principle for web applications, cloud-native computing involves key issues throughout its life-cycle, encompassing building, orchestration, operation, and maintenance. The foundational necessities for cloud-native applications include robust resource management (virtualization and elastic provisioning), security, performance, and efficiency, with performance metrics analyzed at infrastructure, platform, and software levels. The shift from monolithic applications to microservices architecture, supported by DevOps and CI/CD pipelines, is a defining aspect, enabling productivity and continuous deployment. Challenges include service orchestration for diverse applications and managing resources across single-cloud, multi-cloud, and cloud-edge synergy paradigms.

IoT and Smart City Networks: Cloud computing-enabled Internet of Things (IoT) and smart city networks face increasing security and privacy issues due to their constrained application environments. These papers provide comprehensive security analyses, covering various threats, vulnerabilities, consequences, and countermeasures, emphasizing the challenges in ensuring integrity, confidentiality, availability, and non-repudiation in these dynamic settings. The need for lightweight key exchange algorithms and the integration of Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) across all cloud layers are identified as critical future research areas.

Quality Assurance (QA): Cloud computing presents particular challenges associated with quality assurance and validation of software requirements and stability. Current QA frameworks are usually poorly defined, manual, and rigid which often leads to inconsistencies in service delivery and efficiency.

Quantum Cloud Systems: This emerging domain is acknowledged as presenting specific security threats, particularly at the classical-quantum interface, as well as single-tenant, multi-tenant, insider attacks, quantum hardware attacks, and classical component attacks. Proposed mitigation strategies and secure solutions highlight the ongoing need for research in vulnerability assessment and the development of robust cryptographic algorithms to secure this frontier [8].
In conclusion, these papers collectively underscore that while cloud computing presents significant advantages and continues to evolve with new paradigms like serverless and cloud-native, its effective and secure implementation necessitates continuous innovation in security measures, systematic approaches to migration and quality assurance, and a proactive research agenda to address the myriad of challenges and ensure compliance with regulatory frameworks [9].

LITERATURE SURVEY

The literature surrounding cloud computing is extensive and continually evolving, reflecting its foundational role in modern digital infrastructure and its diverse applications across various industries. The provided research papers collectively offer a multi-faceted survey of this domain, encompassing its core definitions, the transformative potential of related technologies, pervasive security challenges, and the strategic implications of its ongoing development [1]. At its core, Cloud Computing (CC) is described as a technology that delivers services to clients over the internet, enabling them to rent necessary services via web browsers [2]. This paradigm is characterized by pervasive features such as online storage, high scalability, and seamless accessibility, which significantly reduce capital costs and workforce requirements for organizations [3]. The architecture typically involves layers, including a hardware layer for physical resource management (routers, cooling systems, servers, switches, power equipment) and an infrastructure layer that uses virtualization technologies like Xen, KVM, and VMware to create storage and computing resource pools [4]. Cloud services are typically divided into the three service models, Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), all of which involve differing degrees of control by the user and management by the provider [5]. While these three service models are generally regarded as the most important, there are also

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

deployment models like the private, public, and community clouds. A significant area of focus across the literature is the interaction between cloud computing and **Big Data** [6]. Big Data refers to datasets that are too massive, heterogeneous, and complex to be efficiently stored, managed, and analyzed using traditional database methods, thereby necessitating scalable architectures for their manipulation and analysis [7]. These vast datasets originate from myriad sources such as smartphones, social media, sensors, point-of-sale terminals, and wearables [8]. Big Data is characterized by various "Vs," including Volume, Velocity, Variety, Veracity, Value, Variability, Volatility, and Vulnerability. Industries like healthcare, automobile, finance, and transportation heavily rely on this data for business strategies and improved decision-making. Efficient processing and storage of Big Data applications in cloud environments remain a primary objective for many research efforts. Data stores must handle large volumes and diverse formats, deliver high performance, and scale dynamically, leading to alternatives like NoSQL and NewSQL databases.

The increasing adoption of cloud services has amplified the criticality of Security concerns, which are proportional to cloud usage. Traditional security measures are often deemed inadequate against the sophisticated and dynamic nature of cyber threats in cloud environments [10]. Research highlights that a large percentage of cyberattacks exploit human behaviors, and data breaches incur substantial costs globally [1]. To bolster cloud security, Deep Learning (DL) and Machine Learning (ML) techniques have emerged as powerful tools capable of analyzing massive volumes of cloud data to identify patterns and abnormalities indicative of security breaches [2]. These techniques are applied to various security challenges, including anomaly detection, security automation,
cloud-native security, image-based malware detection, network traffic analysis, and insider threat detection [3]. Despite the growing interest in ML and DL for cloud security since 2006 (for ML) and 2014 (for DL), challenges persist, notably concerning data privacy, scalability, explainability, generalization, label bias, and integration issues. Addressing these challenges requires developing new algorithms, ensuring compliance with relevant laws and regulations, and employing robust data encryption and access control mechanisms [4].

Several evolving cloud computing paradigms and strategic considerations are also explored: Serverless Computing: Also known as Function-as-a-Service (FaaS), this is a relatively new and exciting field gaining importance due to its ability to reduce costs, decrease latency, improve scalability, and eliminate server-side management. This paradigm allows developers to focus solely on business logic, as providers manage underlying hardware and software. Popular platforms include AWS Lambda, Apache OpenWhisk, and Azure Functions. Serverless computing finds applications in chatbots, information retrieval, file processing, smart grids, security, networks, and IoT. However, it faces challenges such as performance issues, the "cold start" problem (initialization delay for inactive functions), security concerns (due to shared platforms), and a current lack of comprehensive debugging and monitoring tools. Future research aims to overcome cold start issues and develop automated or semi-automated, AI-based migration solutions for legacy systems [3].

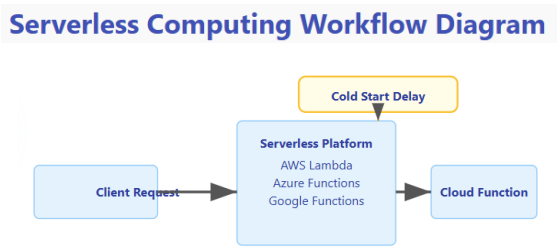

Figure. 1

Cloud Migration: Moving mission-oriented enterprise applications to cloud environments is identified as a significant IT strategic task necessitating a systematic approach. Existing cloud migration approaches are reviewed, focusing on their common characteristics, activities, recommendations, and techniques. Legacy applications, often massive and long-term business investments, encapsulate critical business processes and organizational knowledge. Challenges include a lack of sound research quality in proposed methodologies, insufficient support for multi-tenancy and elasticity (key cloud-specific features), and the absence of a unified process model for migration.

Evaluating migration approaches often involves both generic criteria (e.g., process clarity, tool support) and cloud-specific criteria (e.g., understanding legacy applications, enabling multi-tenancy) [5].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

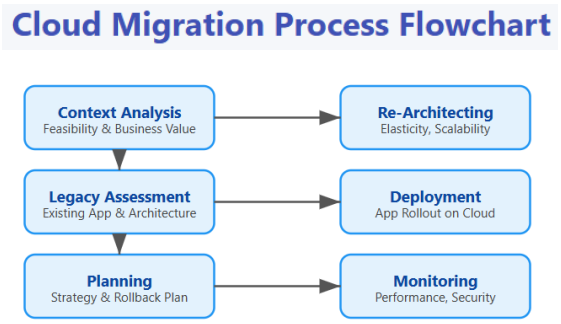

Figure. 2

Cloud-Native Computing: Described as the most influential development principle for web applications, cloud-native computing involves key issues across its life-cycle: building, orchestration, operation, and maintenance. It emphasizes decoupling monolithic applications into loosely-coupled, fine-grained microservices, supported by DevOps and Continuous Integration/Continuous Delivery (CI/CD) pipelines for productivity and continuous deployment. Fundamental necessities include robust resource management (virtualization and elastic provisioning), security, performance, and efficiency. Performance metrics are analyzed at infrastructure, platform, and software levels, covering aspects like resource utilization, failure rates, scalability, reliability, and service-level objectives (SLOs). Service orchestration, essentially container orchestration (e.g., Kubernetes), is crucial for coordinating microservices, with solutions varying based on application types (Machine Learning, High-Performance Computing, Serverless, Batch Jobs) and cloud deployment models (single-cloud, multi-cloud, cloud-edge synergy). Service operation involves load balancing and resource auto-scaling (horizontal and vertical), while service maintenance focuses on data collection, analysis, prediction of future states, anomaly detection, and failure recovery [6].

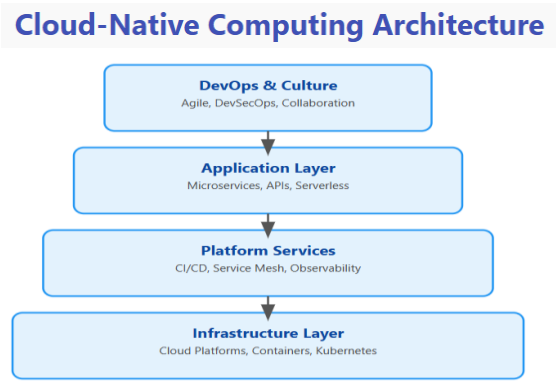

Figure. 3

IoT and Smart City Networks: Cloud computing-enabled Internet of Things (IoT) and smart city networks face increasing security and privacy issues due to their constrained application environments. Comprehensive security analyses cover threats, vulnerabilities, consequences, and countermeasures, emphasizing privacy and trust. Concerns include data over-collection from mobile apps, privacy paradox in online behavior, and the need for robust measures against threats like IP spoofing, DDoS attacks, phishing, and malware. Countermeasures range from "sensing as a service" models with data anonymization to cryptographic mechanisms and privacy-preserving frameworks. Future research in this domain points towards the integration of Artificial Intelligence (AI) and Deep Learning (DL) techniques for enhanced cyber security attack analysis and proactive threat mitigation [7].

Quality Assurance (QA): Cloud computing introduces specific challenges for stable and uniform quality assurance and validation of software requirements. Existing QA frameworks are often criticized for being poorly defined, lacking automation and flexibility, which can lead to inconsistencies in service delivery and efficiency issues [8].

Emerging Technologies: The potential of emerging technologies like blockchain and quantum computing is being explored in cloud security frameworks. Blockchain can enhance data integrity and transparency, while quantum-resistant cryptography aims to protect sensitive data and ML models against future quantum threats. Secure multi-party computation and homomorphic encryption are also being investigated to enable private data analysis and collaborative model building [9].

In summary, the provided literature presents cloud computing as a dynamic and indispensable technology. While it offers profound advantages in scalability, cost reduction, and accessibility, its continued development is heavily dependent on addressing complex challenges, particularly in security, efficiency, and the integration of novel computing paradigms. The ongoing research highlights a clear need for continuous innovation, systematic development methodologies, and adaptive security strategies to realize the full potential of cloud computing across its diverse applications [10]. The Evolving Landscape of Data Storage in the Age of Smart Technologies

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

The explosion of data from smart technologies like IoT, AI, 5G, and cloud computing—forecasted to reach 175 zettabytes per year by 2025—will overwhelm the data storage systems of yesteryear. Cloud storage offers a popular scalable and virtual alternative, and research is primarily on reliability and security as well as all aspects of data management.

While solutions like cryptographic algorithms, PKI, attribute-based access control, and trusted time-stamping have been proposed to tackle issues such as data confidentiality, integrity, access control, dynamic data handling, and data locality, challenges remain. The literature points to ongoing hurdles in practical cloud deployment, including high costs, virtualization vulnerabilities, and difficulties in effectively implementing Service Level Agreements (SLAs) [4].

Recent research consistently emphasizes the vital role of effective quality assurance (QA) in cloud computing. Studies highlight various challenges and proposed solutions for ensuring reliable and secure cloud services. Key concerns include data security risks, a lack of standardized QA methodologies impacting scalability, and the need for robust quality measurement standards and frameworks like ITIL and ISO. Innovative approaches are emerging, such as QA as a Service (QAaaS), which integrates tools and customer feedback (Bernardo et al., 2024). Technical considerations like AAI, FAIR data principles, and workload management are also crucial.Furthermore, broader research explores QA in specific domains, including hybrid cloud models, healthcare applications, and AI-powered manufacturing QA systems. Taken together, the studies prepare and call for a consolidated and flexible QA model for cloud systems. This is necessary in order to meet the performance, security, and legislate concerns that arise from a cloud environment [7].

The rise of quantum cloud computing has brought security to the forefront, particularly concerning multi-tenancy, side-channel attacks, and classical-quantum interface vulnerabilities.

Prior work detailed side-channel attacks on superconducting quantum computers, noting how power, timing, and crosstalk compromise circuit confidentiality. However, it barely touched on multi-tenant threats. We showed SFQ circuits can leak information via bias current analysis, but its implications for shared environments remain largely unexplored. For multi-tenancy, we demonstrated how crosstalk and resource sharing in NISQ systems can be weaponized to reconstruct circuits or disrupt execution. Practical defenses are still mostly theoretical or too costly. Further research on QCaaS architectures and fingerprinting for provider malpractice highlights concerns about platform decisions and authenticity. Despite various proposals, a scalable, practical solution for user confidentiality and system integrity in multi-tenant quantum environments is still missing [9].

DISCUSSION AND ANALYSIS

The provided research papers offer a comprehensive discussion and analysis of various facets of cloud computing, encompassing its fundamental definitions, its interplay with other transformative technologies like Big Data and Artificial Intelligence, critical security concerns, and evolving paradigms such as serverless and cloud-native computing [1].

1. Cloud Computing Fundamentals and Evolution

Cloud computing is perpetually typified as a type of technology that supplies services to customers over the internet and allows the customer to rent the required services using web browsers. Its ubiquitous characteristics such as online storage, considerable scaling, and seamless access will significantly lower capital expenses and reduce employees [2].

The historical context of cloud computing traces back to Leonard Kleinrock's 1969 prediction of "computer utilities," followed by the emergence of grid computing in the 1990s, and gained significant attention with the collaboration between Google and IBM in October 2007. This evolution has led to a structured architecture, commonly categorized by service models and deployment models [3].

Service Models:

Software as a Service (SaaS): Offers subscription-based access to software applications. Users have no control over the underlying infrastructure or application functionality, making it "easy" to use at the "user level". Examples include Salesforce.com, Google Docs, Gmail [4].

Platform as a Service (PaaS): Allows a developer to build, run, and manage applications in the cloud, the user controls the application and its data, the provider controls the runtime, middleware, operating system, virtualization, servers, storage, and networking. PaaS is located in the middle of the flexibility scale. Some examples are Google App Engine and Microsoft Azure [5].

Infrastructure as a Service (IaaS): Gives consumers access to raw hardware-related resources such as CPUs, storage, and memory. Users have the most control over these resources, managing them directly. This model is considered "hard" in terms of difficulty but offers the "most flexible" control. Examples include Amazon EC2 [6].

Deployment Models: Public, private, and community clouds are the common deployment models.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

2. Big Data in Cloud Environments

Big Data refers to datasets that are too massive, heterogeneous, and complex to be efficiently stored, managed, and analyzed using traditional database methods, thus necessitating a scalable architecture. This data can come from many different sources, including smartphones, social media, sensors, point-of-sale terminals, and wearables. The Vs of Big Data are: Volume, Velocity, Variety, Veracity, Value, Variability, Volatility, Vulnerability, and these datasets are made sense of using visualization as one of the reporting methodologies. The industries that maintain Big Data with their business strategies and decision-making processes include health care, automobile, finance, and transportation [7].

Cloud computing has significantly advanced Big Data processing by providing essential computational, networking, and storage capacities. Modern databases need to handle large volumes and diverse formats, deliver high performance, and scale dynamically, which has led to the development of alternatives like NoSQL and NewSQL databases. Key tools and techniques for processing Big Data in cloud environments include HDFS for storage, MapReduce for distributed processing, YARN for cluster resource management, and Zookeeper for coordination services [8].

Despite the opportunities, challenges persist in processing Big Data, particularly due to the dynamic and complex nature of raw data that needs to be processed to extract value. Data curation and the coordination between processing tasks and data are also critical challenges [9].

3. Security in Cloud Computing: The Role of ML and DL

The increasing adoption of cloud services has led to a proportional increase in security concerns. Traditional security controls often cannot keep pace with the evolving sophistication of cyber threat activity, especially in a cloud environment. Some statistics articulate the implications: 84% of successful cyberattacks typically take advantage of human actions, and the average breach in the United States costs $4.1 million. Annual cybercrime costs are projected to exceed $10.5 trillion globally by 2025 [10].

Role of Machine Learning (ML) and Deep Learning (DL): ML and its subset, DL, have emerged as powerful tools for enhancing cloud computing security. These techniques can analyze massive volumes of cloud data to identify patterns and abnormalities indicative of security breaches. ML models, by learning from historical data, enable proactive threat identification, distinguishing between harmful and regular activity. DL further refines this by using neural network architectures to automatically extract complex features for more precise detection [1].

Key Trends in ML/DL for Cloud Security:
Anomaly Detection: Involves recognizing patterns or events that deviate from normal system activity in the case of real time detection, efficient use of cloud data, resource optimizations, and different ML algorithms, is likely to improve accuracy [2].

Security Automation: Focuses on automating security tasks, such as incident response, threat intelligence visualization, policy enforcement, security orchestration, and predictive modeling. DL contributes to automating anomaly detection, incident response, self-learning, and root cause analysis [3].

Cloud-Native Security: Integrates security measures directly into cloud environments to protect cloud-native applications and data. This involves cloud-native network security solutions, centralized management platforms, and policy management, considering multi-tenancy and dynamic resource allocation challenges [4].

Role of Emerging Technologies: Investigating new and emerging technologies to enhance security. We are looking into Blockchain to contribute to data integrity and transparency and Quantum-resistant cryptography for the preservation of sensitive data and ML models that may be threatened in the future. Secure multi-party computation and homomorphic encryption enable private data analysis and collaborative model building. Zero-trust network access models are also being explored [5].

ML-Specific Foci: Include detecting insider threats through behavioral detection, user profiling, natural language processing (NLP), and graph analysis. It also covers security brokers for identity and access management, data loss prevention, threat protection, and compliance management [6].

DL-Specific Foci: Predominantly involve image-based malware detection (analyzing malware behavior, classification, variant detection, visualization, and image compression) and network traffic analysis (classification, traffic flow analysis, and manipulation for efficiency) [7].

Challenges of ML/DL for Cloud Security: Despite their promise, ML and DL in cloud security face significant challenges:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

Data Privacy: Training models require large volumes of data, which must be protected, especially in shared cloud infrastructures. Solutions include
robust data encryption, access control, differential privacy, and federated learning [8].

Scalability: Ensuring ML/DL models can handle the massive and growing scale of cloud data and operations [9].

Explainability: Difficulty in producing clear decision-making logic from complex models, necessitating better documentation of model training and evaluation [10].

Generalization: Models struggle to generalize to new, unseen attack types. Augmenting training datasets, using transfer learning, and frequent model updates are recommended [1].

Label Bias and Integration Issues: These also pose obstacles to effective implementation [2].

Compliance: Developing algorithms and techniques that comply with relevant laws and regulations is essential for effective implementation [3].

Future research in this area calls for further investigation into automated incident response, image-based malware detection, cloud-native security, and the application of ML/DL in edge/fog computing and IoT-based data processing [4].

4. Cloud Migration Processes

Moving mission-oriented enterprise applications to cloud environments is a major IT strategic task that requires a systematic approach. Legacy applications are recognized as massive, long-term business investments that encapsulate critical business processes and organizational knowledge. The motivation for migration stems from the need for high computing capability, scalability, and resource consumption, with the global cloud computing market projected to grow significantly [5].

Challenges in Cloud Migration Methodologies: A significant finding from the surveys is the "lack of sound research quality" in many proposed methodologies, with very few adequately detailing their research design, data collection, or analysis techniques. This undermines the trustworthiness and combinability of existing approaches. Other critical gaps include:

Insufficient Support for Cloud-Specific Features: Many approaches lack adequate support for multi-tenancy, elasticity, and comprehensive testing with continuous integration (CI).

Undefined Developer Roles: The definition and responsibilities of roles involved in the migration process are often not well described, despite the emergence of new, cloud-specific skills.

Weak Support for Key Methodological Aspects: Traceability, scalability, formality, and automation are weakly supported by existing approaches [6].

Evaluation Framework and Key Activities: To address these shortcomings, an evaluation framework has been proposed, categorizing criteria into "generic" (e.g., process clarity, tool support, modeling language, traceability, work-products) and "cloud-specific" (e.g., analyzing context, understanding legacy application, enabling multi-tenancy/elasticity, test and continuous integration, continuous monitoring) [7].

Key activities highlighted in migration literature include:
Context Analysis: Assessing feasibility and business value of cloud adoption, investigating concerns like user resistance, loss of governance, security risks, legal restrictions, and cost.

Understanding Legacy Application: Recapturing an "As-Is" representation of application architecture, including functionality, dependencies, and code quality. This is crucial for automatic transformation and cost estimation.

Elasticity: Elasticity is often conceptual, and while there is not always clear methodology underlying it, enabling elasticity often involves specifying a description of compute resources, application lifecycle and scaling rules, and automatic provisioning and implementation and performance monitoring.

Continuous Integration: Continuos integration is an important prerequisite without which integration will proceed badly. This could involve environment set up of staging and production to check that you check new increments will be integrated smoothly.

Future Research in Cloud Migration: Future research should focus on improving the research rigor of methodologies, enhancing support for multi-tenancy and elasticity, refining developer roles, strengthening traceability, scalability, and automation, and developing a generic reference model to integrate the fragmented body of knowledge in cloud migration [8].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

5. Serverless Computing Paradigm

Serverless computing, also known as Function-as-a-Service (FaaS), has gained significant importance due to its ability to reduce costs, decrease latency, improve scalability, and eliminate server-side management for developers. In this paradigm, developers focus solely on business logic, while providers manage the underlying hardware and software infrastructure [9].

Key Characteristics and Platforms: A defining characteristic of serverless is "scaling to zero," meaning functions remain idle when not requested, which saves costs but introduces the "cold start" problem. Popular commercial platforms include AWS Lambda, Google Cloud Functions, and Azure Functions, while open-source options include Apache OpenWhisk and IBM Cloud Functions. Applications range from chatbots and information retrieval to smart grids, security, networks, IoT, and edge computing [10].

Challenges of Serverless Computing:
Cost and Pricing Model: A fundamental challenge, as providers need to minimize resource usage, and pricing models can be complex depending on function types (e.g., CPU-bound vs. I/O-bound) [1].

Cold Start Problem: The time it takes for the first invocation of an idle function due to starting up (initialization) that shows a significant opportunity for optimization [2].

Resource Limits: Limitations related to CPU, memory, execution time and bandwidth [3].

Security: Considered the "most challenging issue," especially regarding isolation due to functions running on shared platforms and trust concerns with sensitive data [4].

Programming and Debugging Tools: A current lack of comprehensive debugging and monitoring tools, as well as advanced integrated development environments (IDEs), hinders development [5].

Vendor Lock-in: A problem identified with serverless providers, limiting flexibility across different platforms [6].

Future Research Directions in Serverless Computing: Future research aims to overcome the cold start problem through enhanced scheduling policies and accurate performance measurements. Additionally, decomposing and migrating legacy systems to FaaS without performance degradation is a key area, particularly developing optimal automated and semi-automated, AI-based migration solutions [7].

6. Cloud-Native Computing Paradigm

Cloud-native computing (CNC) is identified as the most influential development principle for web applications, evolving from Service-Oriented Architecture (SOA) and emphasizing microservices architecture. This approach decouples monolithic applications into loosely-coupled, fine-grained microservices, supported by DevOps and Continuous Integration/Continuous Delivery (CI/CD) pipelines for enhanced productivity and continuous deployment [8].

Life Cycle and Fundamental Necessities: The life cycle of cloud-native applications is divided into four states: building, orchestration, operation, and maintenance. The foundation of CNC lies in robust resource management through virtualization and elastic provisioning, ensuring business agility. Security, performance and efficiency are main general function modules [9].

Performance Metrics: Performance in CNC is analyzed at three levels:

Application Level: Measured by Quality of Service (QoS), latency, response time, completion time, and makespan.

Platform Level: Focuses on reliability (system's ability to deliver services without disruption), throughput, scalability, fairness, and cost, often optimized through load balancing, resource allocation, and scheduling.

Infrastructure Level: Concerned with resource utilization (computation, storage, network), failure rates, interference, and energy consumption of raw computing resources [10].

Service Orchestration: This involves the automated configuration, management, and coordination of microservices, primarily through container orchestration tools like Kubernetes. Solutions vary based on application types and computational architectures:

Application Types: Include Machine Learning (model training and inference), High-Performance Computing (HPC) jobs, Serverless Computing (managing interdependencies among functions), and Batch Jobs (optimizing scheduling and resource utilization).

Cloud Types: Single-cloud, multi-cloud (sharing resources for reliability and cost reduction), and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

cloud-edge synergy (processing data at the network edge to reduce latency and energy consumption).

Service Operation: Crucial for maintaining system performance and efficiency, involving:

Load Balancing: Techniques to prevent overloading a single container or cluster, ensuring optimal resource utilization.

Service Migration: Optimizing the movement of virtual machines (VMs) and containers, considering factors like latency, energy consumption, and prediction accuracy [1].

Resource Auto-Scaling: Dynamically adjusting resources horizontally (adding/removing VMs) for cost-efficiency and fast scaling, and vertically (adjusting resources within a VM) for optimizing cost and efficiency for varying workloads [2].

Service Maintenance: This state focuses on collecting and analyzing service and system indicators, adjusting strategies, and performing fault recovery. It includes data collection (monitoring physical infrastructure and service performance), data analysis (summarizing characteristics, predicting future states, anomaly detection, root cause analysis), and failure recovery mechanisms (redundancy, failover, and repair) [3].

Challenges and Opportunities in CNC: Despite its advancements, CNC still lacks a clear research roadmap and comprehensive systematic knowledge for ensuring portability and compatibility across diverse applications. A specific challenge relates to data distribution in data-driven models, where a trade-off exists between training a single model for all servers (cost-efficient) versus individual models (more accurate). Continuous innovation is needed to create more efficient, secure, and scalable software systems [4].

Conclusion of Analysis

The research papers collectively highlight that cloud computing, while a powerful and indispensable technology underpinning modern digital infrastructure, is in a continuous state of evolution. The integration with Big Data and the increasing reliance on ML/DL for security demonstrate the growing complexity and interdependency of these technologies. The detailed discussions on cloud migration, serverless computing, and cloud-native computing reveal a shared emphasis on optimizing performance, scalability, and cost-efficiency, alongside a persistent struggle with security, operational challenges, and the need for more systematic methodologies. The identified gaps in current research, particularly regarding automation, robust validation, comprehensive tool support, and nuanced security strategies, provide clear directions for future advancements. These sources underscore that realizing the full potential of cloud computing requires continuous innovation, interdisciplinary collaboration, and a diligent focus on addressing the intricate technical and methodological challenges that arise in these dynamic environments.

Cloud Storage: Security and Management Challenges

Cloud storage presents two primary challenges: Data Security and Data Management.

Security Issues encompass confidentiality, integrity, access control, authentication, and breaches. While methods like encryption, proxy re-encryption, PKI, and trusted timestamping offer solutions, Attribute-Based Encryption (ABE), specifically CP-ABE and KP-ABE, provides fine-grained access control but can add computational overhead.

Data Management Issues involve data dynamics, segregation in multi-tenant environments, virtualization vulnerabilities, data backup, availability, and data locality. Multi-tenancy and virtualization raise concerns about isolation and data leakage. Proposed solutions include root security, multitier architecture, and region-specific backups, but their real-world implementation faces hurdles in scalability, regulatory compliance, and integration.

Ultimately, while comprehensive strategies exist, practical cloud implementations demand careful consideration of trade-offs among cost, complexity, and performance [4].

The realm of cloud quality assurance (QA) faces significant hurdles, primarily due to the absence of standardized protocols and a reliance on inefficient manual processes. Another major challenge lies in the difficulty of maintaining consistent performance as cloud resources scale up or down. Furthermore, QA practices tend to vary widely across different organizations and platforms, creating inconsistencies. Recognizing these gaps in current research and practice, the authors propose an integrated, automated, and flexible QA approach. This framework's effectiveness is supported by a descriptive statistical analysis of survey data gathered from 30 industry practitioners [7].

Multi-tenant quantum clouds face significant vulnerabilities. Crosstalk is a key attack vector, easily compromising circuit confidentiality. Side-channel attacks (timing, power) also exploit subtle execution characteristics.The classical-quantum interface presents attack surfaces due to hardware flaws, exacerbated by insider threats and weak access controls.Current mitigations are partial, highlighting a performance-security trade-off, especially for NISQ devices.Multi-tenancy, while boosting accessibility, inherently compromises security. Many providers lack sufficiently hardened

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

infrastructure due to cost focus. Future secure QCaaS demands empirical validation of defenses, integrating zero-trust, real-time auditing, and advanced quantum-safe encryption [9].

METHODOLOGY

This paper presents a survey of key issues during the lifecycle of cloud-native applications, specifically from the perspective of services [1]. It organises the research domains by decoupling the cloud-native application lifecycle into four states: building, orchestration, operate, and maintenance [2]. The survey also describes key requirements and summarises important performance metrics. It aims to merge industrial popularity with trending academic research [3].

The methodology involves:

Focus on Service Lifecycle: The survey analyses key problems across the entire lifecycle of cloud-native applications, from the building state to the maintenance state [4].

Performance Metrics and Fundamental Necessities: It discusses performance metrics and the fundamental necessities required when developing cloud-native applications [5]. These include resource management (resource virtualisation and elastic provisioning) as the central issue, and general function modules focusing on security, performance, and efficiency [6].

Review of Virtualisation Technologies: It reviews different types of virtualisation (computation, storage, network) and their role in cloud-native design and deployment [7].

Service Orchestration: This section describes the automated configuration, management, and coordination of multiple microservices to deliver end-to-end services, essentially focusing on container orchestration [8]. It classifies orchestration solutions based on application types (Machine Learning, High-Performance Computing (HPC), Serverless Computing, Batch Jobs) and computational architectures (Single-Cloud, Multi-Cloud, Cloud-Edge Synergy) [9].

Service Operation: This state encompasses load balancing, service migration, and resource auto-scaling, which are crucial for maintaining a high-performing and efficient system infrastructure. Load balancing techniques and their implementation, and VM-based versus container-based service migration are reviewed. Auto-scaling policies are summarised into horizontal and vertical scaling approaches [10].

Service Maintenance: This involves collecting and analysing service and system indicators, adjusting and developing strategies, and performing fault recovery. Data collection from physical infrastructure and services (temporal and operation contexts) is discussed. Data analysis focuses on summarising characteristics, predicting future states, and detecting anomalies and root causes, utilising various statistical and learning-based methods [10].
The paper claims to be the first survey to examine important concerns during the life of cloud-native applications from the services viewpoint, rather than a high-level general opinion or a focused coverage of particular issues in cloud-native computing. It aims to provide enlightening thoughts and stimulate future research directions [10]. This study systematically surveys recent developments, obstacles, and remedies within cloud storage architecture. We've thoroughly examined peer-reviewed research, whitepapers, industry reports, and relevant standards.

Our approach involved:

Categorizing issues into two main areas: data security and data management.

Delving into sub-categories such as access control, various encryption methods, the enforcement of Service Level Agreements (SLAs), and backup mechanisms.

Benchmarking existing solutions against key metrics like performance, security levels, and scalability.

Pinpointing gaps in current models, with a particular focus on challenges related to multi-tenancy, regulatory compliance, and virtualization vulnerabilities.

The analysis is qualitative and descriptive, intending to provide valuable insights for future researchers and system designers in this evolving field [4].

This study's methodology involved designing a new QA framework built upon three core pillars: Standardization, Automation, and Adaptability. For validation, we used a structured questionnaire survey. We collected quantitative data from a sample of 30 cloud computing professionals, randomly selected from the industry, using Likert scale responses. The data was then analyzed using descriptive statistics, cumulative frequencies, and bar chart visualizations [7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

This study adopts a survey-based qualitative methodology to critically examine existing literature on security threats in quantum cloud computing, with a particular focus on multi-tenancy and the classical-quantum interface.

Our approach involved the following steps:
Literature Collection: We reviewed peer-reviewed articles, arXiv preprints, and IEEE papers from 2015–2025, using sources like IEEE Xplore, Springer, and arXiv. Selection criteria emphasized threats in Quantum Computing as a Service (QCaaS), especially side-channel attacks, classical-quantum interface vulnerabilities, and multi-tenant models.

Thematic Categorization: Collected works were organized into six main themes: Quantum Cloud Architecture, Multi-Tenancy Threats, Classical-Quantum Interface Attacks, Side-Channel Exploits, Proposed Solutions, and Research Gaps.

Comparative Analysis: Key findings were cross-referenced and analyzed for threat level, feasibility, and impact on confidentiality, integrity, and availability (CIA triad), revealing patterns and research gaps.

Visual Frameworks: Diagrams and summary tables (e.g., Fig. 2 and Table II) were used to represent threats, attack vectors, and security impacts for clearer conceptualization.

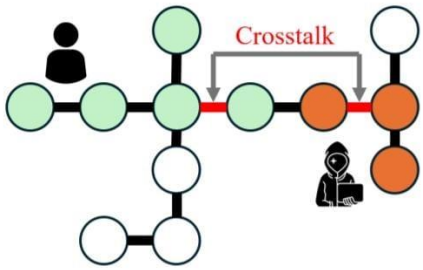

Fig. 2: Crosstalk-Channel Attack on a Quantum System

Fig. 2

TABLE II: Types of threats and their damage possibility stemming from the primary goals of the exploits on multi-tenant quantum cloud systems, focusing on their effects on the CIA Triad (confidentiality, integrity, and availability).

Research Papers	Confidentiality	Integrity	Availability	Threat Level
Crosstalk Side Channels [6]	Yes	Yes		High
Active SWAP Attack [19]		Yes	Yes	Moderate
Passive SWAP Attack [19]	Yes			High
Reset Operation Threats [33]	Yes			Moderate
Reconstructing Circuits [34]	Yes			Moderate
Qubit Flipping Attacks [35]		Yes		High

Table II

Gap Identification: We conclude by identifying critical research needs—especially practical, low-overhead security protocols—and call for cross-disciplinary efforts to develop scalable protections for quantum cloud system [9].

CONCLUSION

The provided research papers offer a comprehensive overview of cloud computing, its evolving paradigms, inherent challenges, and future opportunities, with a particular emphasis on security and migration. Cloud computing is a widely adopted information services delivery model that provides scalable, elastic, on-demand, and pay-per-use access to pooled computational resources like storage, servers, and applications over the Internet. It eliminates the need for users to manage the underlying infrastructure, offering benefits such as cost reduction, decreased latency, improved scalability, and simplified deployment. Key service models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), which are fundamental to its operation. In conclusion, the progression of cloud computing is characterized by a continuous push towards more flexible, scalable, and automated service delivery models like cloud-native and serverless computing. This evolution is intrinsically linked with the parallel development and application of advanced AI/ML/DL techniques, primarily to enhance security, optimize performance, and streamline operations. Despite notable progress, the inherent complexities of distributed environments, particularly concerning data privacy, security threats, and the need for standardized, robust migration and management methodologies, present ongoing challenges that necessitate continued research and innovation.

REFERENCES

1. Muniswamaiah, M., Agerwala, T., & Tappert, C. (2019). Challenges of Big Data Applications in Cloud Computing. International Journal of Computer Science & Information Technology (IJCSIT), 11(4), 221-232. doi:10.5121/csit.2019.90918
2. Bokhari, M. U., Shallal, Q. M., & Tamandani, Y. K. (2018). A Survey on Cloud Computing. In V. B. Aggarwal et al. (Eds.), Big Data Analytics, Advances in Intelligent Systems and Computing (Vol. 654, p. 149). Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-10-6620-7_16
3. Fahmideh, M., Low, G., Beydoun, G., & Daneshgar, F. (The exact publication year of this "author's copy" is not explicitly stated in the provided excerpt, but it has been accepted and published in the Journal of Systems and Software (JSS), covering literature up to 2015). Cloud Migration Process: A Survey, Evaluation Framework, and Open Challenges.
4. Ghani, A., Badshah, A., Jan, S. U., Alshdadi, A. A., & Daud, A. (2020). Issues and challenges in Cloud Storage Architecture: A Survey. Researchpedia Journal of Computing, 1(1), 50–65.
5. Hassan, H. B., Barakat, S. A., & Sarhan, Q. I. (2021). Survey on serverless computing. Journal of Cloud Computing:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 07, July - 2025

Advances, Systems and Applications, 10(39). https://doi.org/10.1186/s13677-021-00253-7

6. Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., & Kim, K.-I. (2021). A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges. Electronics, 10(15), 1811. https://doi.org/10.3390/electronics10151811
7. Qureshi, R., & Alharbi, M. A. (2025). Issues and Challenges in Quality Assurance Process of Cloud-Based Software Development: A Systematic Literature Review. International Journal of Software Engineering & Applications (IJSEA), 16(1)1819
8. Deng, S., Zhao, H., Huang, B., Zhang, C., Chen, F., Deng, Y., Yin, J., Dustdar, S., & Zomaya, A. Y. Cloud-Native Computing: A Survey from the Perspective of Services. (This paper is presented as a survey from the perspective of IEEE members; the specific journal and exact publication year are not provided in the excerpt)
9. Nguyen, H. T., Krishnan, P., Krishnaswamy, D., Usman, M., & Buyya, R. (2024). Quantum cloud computing: a review, open problems, and future directions. arXiv preprint arXiv:2404.11420
10. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57(132). https://doi.org/10.1007/s10462-024-10776-5