Jyoti Nivas College Autonomous

Post Graduate Centre

Department Of Computer Science (PG)

E-Journal

On

Cloud Computing

ISSUE 2

SEPTEMBER 2024

CLOUD COMPUTING BASED INTERNET OF THINGS

TEJASHREE.A (23MCA39)

AYESHA BANU (23MCA05)

Cloud computing is one element that enhances the Internet of Things' success. With cloud computing, users can use online services to complete computing chores. Because cloud computing and the Internet of Things are now interconnected, their use together has become somewhat of a catalyst. These are truly cutting-edge technologies that will have numerous advantages.

The issue of storing, analyzing, and accessing vast volumes of data has emerged as a result of technology's quick development. Utilizing cloud and Internet of Things technology together is a great example of creativity. New monitoring services and advanced processing of sensory data streams will be able to be used together.

Benefits of Integration of IoT and Cloud Computing:

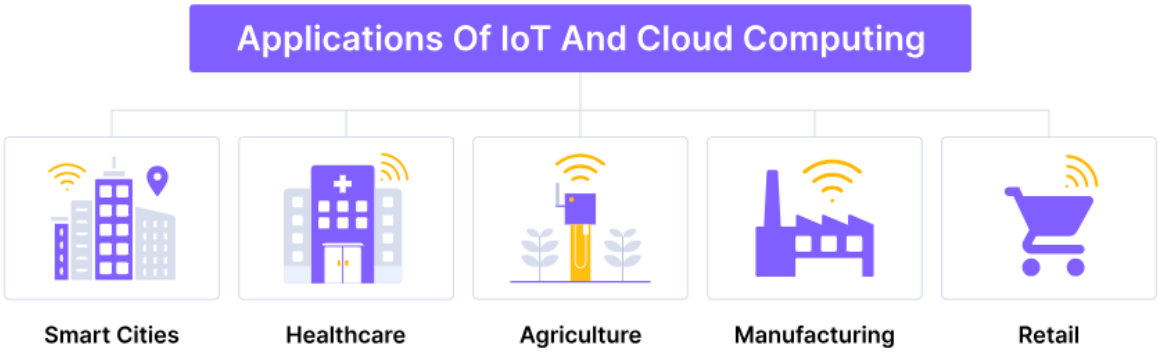
- Scalability:
  Without requiring major infrastructure changes, cloud computing enables IoT systems to scale with ease, managing growing numbers of devices and enormous volumes of data.
- Cost-effectiveness:
  lowers the cost of deploying and maintaining IoT solutions by eliminating the requirement for physical infrastructure and on-site maintenance.
- Processing Data in Real Time:
  allows for the rapid, real-time analysis of data produced by Internet of Things devices, facilitating automation and prompt decision-making.
- Remote Control and Access:
  The ability to remotely monitor and control IoT devices via the cloud gives users the freedom and convenience to oversee operations from any location.
- Integration of AI and Advanced Analytics:
  IoT systems can use cloud computing to take use of strong analytics and artificial intelligence (AI) technologies to improve decision-making, streamline operations, and obtain deeper insights.

Disadvantages of Integration of IoT and Cloud Computing:

- Risks to Security:
  If security is weak, storing private information in the cloud increases the danger of hackers, data breaches, and illegal access.
- Problems with Latency:
  Real-time operations that demand quick reactions may be impacted by communication lags between IoT devices and the cloud.

- Reliance on connectivity to the internet:
  Stable internet connections are essential for cloud-based IoT devices, and any network outages might result in serious system failures.
- Data Privacy Issues:
  Cloud storage of sensitive or identifiable data presents privacy challenges, particularly with regard to GDPR compliance.
- Continuous Expenses:
  As IoT deployments grow in size and data usage, cloud service costs may rise, resulting in higher long-term costs.

IoT and Cloud Computing in Real-World Applications



MULTI-CLOUD: A COMPREHENSIVE REVIEW

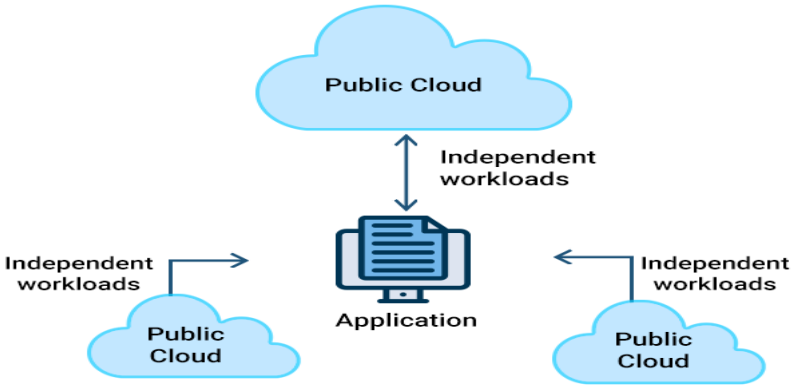
SWETHA R (23MCA37)

C THANU SREE (23MCA11)

Introduction

Cloud computing has fundamentally transformed how organizations deploy and manage their IT infrastructure. The flexibility, scalability, and cost-efficiency of cloud services have led to widespread adoption across industries. However, as organizations seek to avoid dependency on a single cloud provider, multi cloud strategies have gained traction. A multi cloud environment involves the use of services from multiple cloud providers to meet specific business needs.

Multi cloud offers benefits such as increased flexibility, better cost management, and enhanced resilience, but also introduces complexities in management, security, and integration. This paper aims to provide a comprehensive review of multi cloud computing, analyzing its key components, advantages, challenges, and emerging trends.



Benefits of Multi cloud

- **Avoiding Vendor Lock-in:** Multi cloud allows organizations to select the best services from different providers, avoiding dependency on a single vendor.
- **Cost Optimization:** Businesses can optimize costs by choosing providers that offer the most competitive pricing for different services.
- **Resilience and Disaster Recovery:** Distributing workloads across multiple clouds ensures high availability and minimizes downtime in case of a provider's failure.
- **Performance Optimization:** Organizations can choose cloud providers geographically closer to end users to reduce latency and improve performance.
- **Regulatory Compliance:** Multi cloud can help meet regional compliance requirements by selecting specific providers that adhere to local regulations.

Challenges of Multi cloud

- **Management Complexity:** Handling multiple cloud environments can be complex, requiring advanced tools for orchestration, monitoring, and resource management.
- **Security and Privacy Risks:** Different cloud providers may have varying security protocols, complicating the enforcement of consistent security policies across all platforms.
- **Integration Issues:** Integrating applications and data across multiple clouds can be challenging due to differences in APIs, storage mechanisms, and network configurations.
- **Data Transfer Costs:** Transferring data between clouds may incur significant costs, especially when dealing with large volumes of data.

SECURITY AND PRIVACY PROTECTION IN CLOUD COMPUTING

Shwetha V(23MCA33)

Introduction

Cloud computing has transformed the way computing resources, storage, and software are accessed and utilized. It offers scalability, flexibility, and cost-efficiency, enabling applications in fields such as scientific research, education, entertainment, and business. However, the shared and distributed nature of cloud environments introduces significant security and privacy challenges. These include data breaches, unauthorized access, insider threats, and vulnerabilities in virtualization and multi-tenant systems.

The inherent complexity of cloud systems, combined with the outsourcing of data to third-party providers, increases the risk of privacy violations and cyberattacks. Traditional data protection mechanisms are often insufficient in addressing these challenges, necessitating the development of advanced frameworks and technologies to safeguard sensitive data and maintain user trust.

Technologies in Cloud Security

To address the unique challenges posed by cloud environments, the following technologies are highlighted:

1. Access Control Mechanisms: These include traditional models like Discretionary Access Control (DAC) and Role-Based Access Control (RBAC), along with advanced Attribute-Based Access Control (ABAC), which allows for fine-grained permission management.
2. Attribute-Based Encryption (ABE): ABE enables policy-driven, fine-grained control over encrypted data. Subtypes like Key Policy ABE (KP-ABE) and Ciphertext Policy ABE (CP-ABE) allow flexible access management.
3. Searchable Encryption (SE): Supports searching within encrypted data without compromising its confidentiality.
4. Proxy Re-encryption (PRE): Outsources re-encryption tasks to third parties, reducing computational overhead for users.
5. Multi-Authority Systems: Distributes trust among multiple entities to enhance security and prevent single points of failure.
6. Hierarchical Encryption: Offers scalable and flexible encryption, particularly in multi-tiered organizational structures.

Challenges in Cloud Security

Despite advancements in security technologies, cloud computing faces persistent challenges, including:

1. Multi-Tenancy Security: Ensuring isolation and security among tenants sharing the same cloud infrastructure.
2. Attribute Revocation: Addressing the revocation of attributes or permissions in encryption schemes like ABE without affecting other users.
3. Trust Management: Establishing and maintaining trust in multi-domain and multi-authority environments, especially with third-party providers.

4. Insider Threats: Mitigating risks from malicious or negligent actions by individuals within an organization or service provider.
5. Scalability of Security Solutions: Ensuring that security mechanisms scale effectively with increasing data and user volume.
6. Integration of Technologies: Combining access control, encryption, and authentication into seamless, efficient frameworks.
7. Lightweight Security Mechanisms: Developing security solutions optimized for resource-constrained devices and edge computing environments.

By addressing these challenges and leveraging advanced technologies, cloud computing can achieve a secure and privacy-resilient ecosystem that meets the demands of modern applications.

Role of Cloud Computing in Supporting Smart City Infrastructure

Lavanya A (23MCA17)

Nanthini E (23MCA21)

The advancement of urban landscapes into "smart cities" has gained a significant role in recent years that are largely driven by the combination of advanced technologies. One of the core enables smart city infrastructures is cloud computing, which offers a flexible, scalable, systematic or structured way to manage and process the vast amounts of data that has been generated in urban environments. The role of cloud computing in the development, management, and optimization of smart city infrastructures, with a focus on data management, cost-efficiency, security, and scalability. It also inspects the potential provocation and future trends in manipulating cloud computing for smart city applications.

Smart cities generate a large volume of data through IoT devices, sensors, and other technologies. The most effective management of this data is crucial for urban based services such as traffic management, energy optimization and healthcare services.

Smart city aims in improving the quality of life of citizens by creating sustainable implements. The issue of smart city should be considered as a concept that involves various economic, humanitarian or legal elements instead of being seen only as a technological issue. The main purpose of the smart city creativity is to ensure the sustainability of cities, to increase or involve social activities and to facilitate the living conditions.

The understanding provided by cloud-based data analytics enable cities to make informed decisions that positively collides the environment and contribute to a greenery as well as sustainable environment.

It ensures that various components of a smart city ecosystem, such as transportation, public safety, environmental monitoring, and healthcare systems, can work together. By providing this framework for collaboration and interoperability, cloud computing enables smart cities to develop the collective expertise and resources of multiple or various stakeholders, which results in matching and effective approach to address the complex challenges of urban development.

THE IMPACT OF SOCIAL MEDIA ON MENTAL HEALTH: A REVIEW OF THE LITERATURE

Sheba Evangline (23MCA31)

Abstract
Social media has become an integral part of modern life, but its impact on mental health is a topic of growing concern. This paper reviews the existing literature on the relationship between social media use and mental health outcomes, including anxiety, depression, and loneliness.

Introduction
Social media platforms, such as Facebook, Instagram, and Twitter, have become essential tools for communication, self-expression, and social connection. However, excessive social media use has been linked to negative mental health outcomes, including anxiety, depression, and loneliness.

LiteratureReview
Numerous studies have investigated the relationship between social media use and mental health outcomes. A systematic review of 36 studies found that social media use was significantly associated with increased symptoms of depression and anxiety.

Methodology
This study employed a quantitative research design, using a survey to collect data from a sample of 1,000 social media users.

Results
The results of this study found that excessive social media use was significantly associated with increased symptoms of anxiety and depression.

Discussion
The findings of this study support the existing literature on the negative impact of social media on mental health. The constant stream of curated and manipulated content on social media can create unrealistic expectations and promote consumerism, materialism, and narcissism.

Conclusion
The impact of social media on mental health is a complex and multifaceted issue. While social media has the potential to provide social support and connection, excessive use can have negative consequences for mental health.

Cloud Computing and Cryptography

Pallavi P (23MCA23)
Priyanka R (23MCA25)

Introduction

Cloud computing has revolutionized how individuals and organizations access computing resources by providing flexible, scalable, and on-demand services via remote servers. This eliminates the need for local infrastructure, reducing IT costs. Users can access applications, storage, and processing power as needed, allowing businesses to scale resources based on demand. A key benefit of cloud computing is its cost-effectiveness, as organizations only pay for the resources they use. However, security concerns around data privacy and integrity arise from storing sensitive data on third-party servers. Cryptography plays a vital role in ensuring data security by encrypting it, protecting it from unauthorized access.

Types of Cloud ComputingDeployment Models

Private Cloud: Dedicated to a single organization, providing higher control andsecurity over data. It is typically used by large enterprises or government agencies.
Public Cloud: Open to any user, hosted and managed by third-party providers like Amazon Web Services (AWS) and Microsoft Azure. It is cost-effective but may not offer the same level of control or security as private clouds.
Community Cloud: Shared by several organizations with similar needs, offering a balance of security and collaboration. It is common in sectors like healthcare and finance.
Hybrid Cloud: Combines public, private, and community clouds, allowing organizations to utilize the strengths of each model while addressing specific requirements for cost, security, and flexibility.

Service Models

Software as a Service (SaaS): Provides software over the internet, eliminating the needfor local installation. Examples include Google Workspace and Microsoft Office 365.
Infrastructure as a Service (IaaS): Offers virtualized computing resources such as storage and processing power on a pay-as-you-go basis. Providers include AWS and Google Cloud.
Platform as a Service (PaaS): Supplies a platform for developing, testing, anddeploying applications without worrying about the underlying infrastructure. Examplesinclude Google App Engine and Microsoft Azure.

Cryptography in Cloud Computing

Cryptography is essential in cloud computing to ensure data confidentiality and integrity. By converting data into an unreadable format, cryptography protects it from unauthorized access. In cloud computing, there are two primary objectives of cryptography:

Confidentiality: Ensuring that data is only accessible to authorized users.
Integrity: Ensuring that data remains unaltered during storage or transmission.

To achieve these objectives, encryption algorithms are used to transform plaintext data intociphertext, making it unreadable without the decryption key.

Confidentiality: Ensuring that data is only accessible to authorized users.
Integrity: Ensuring that data remains unaltered during storage or transmission.

To achieve these objectives, encryption algorithms are used to transform plaintext data into ciphertext, making it unreadable without the decryption key.

Types of Cryptographic Algorithms

Symmetric Key Cryptography: In this method, the same key is used for bothencryption and decryption. It is fast and efficient, making it suitable for large volumesof data. **AES** (Advanced Encryption Standard) is a widely used symmetric encryption algorithm in cloud computing.
Asymmetric Key Cryptography: This method uses two keys—a public key for encryption and a private key for decryption. While more secure, it is computationally intensive. **RSA** is a popular asymmetric encryption algorithm used in cloud environments.

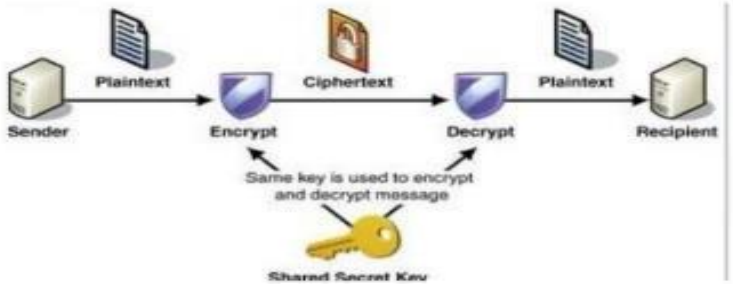
Challenges in Cloud Cryptography

Despite its importance, cryptography in cloud computing faces several challenges:

Key Management: Effective management of encryption keys is crucial for maintainingsecurity. If keys are not stored securely or shared properly, unauthorized access to datacan occur.
Performance and Scalability: Encryption can be resource-intensive, particularlyasymmetric encryption, and may impact cloud service performance. Providers must balance strong encryption with efficient performance.
Data Auditing and Compliance: Encrypted data must remain auditable for compliance with regulations like GDPR or HIPAA. Ensuring that encrypted data is stillaccessible for auditing without compromising security is a key challenge.

Conclusion

Cloud computing provides benefits like cost savings, flexibility, and scalability, but securityis still a major concern, especially for data privacy and integrity. Cryptography is crucial forprotecting data in the cloud, ensuring it remains confidential and intact. Although symmetricand asymmetric encryption methods are widely used, challenges like key management, performance, and compliance must be addressed. As cloud computing evolves, improving cryptographic methods will be key to maintaining the security and privacy of cloud data.



Blockchain-Driven Cloud Data Integrity Protection

Bhargavi S(23MCA08)

Deepthi Shalini D(23MCA12)

Introduction

In today's digital landscape, maintaining the integrity of data housed in cloud environments is crucial, as organizations of all sizes depend on these services for essential operations. However, the widespread occurrence of cyber threats and data breaches has diminished confidence in conventional cloud storage systems, underscoring the pressing need for innovative solutions to safeguard data integrity. Blockchain technology, characterized by its decentralized, immutable, and transparent nature, presents a promising solution to these issues. By implementing blockchain-based approaches, the protection of cloud data integrity can be significantly improved, providing strong verification processes that ensure the authenticity and dependability of stored information. This essay will examine the relationship between blockchain and cloud technologies, demonstrating how the former can strengthen the latter against data manipulation and vulnerabilities, ultimately enhancing user and stakeholder trust in the security of their digital assets.

Overview of Cloud Data Integrity Challenges

Cloud data integrity concerns stem from data corruption and unauthorized access, posing risks for businesses relying on cloud storage. With increasing cloud adoption, data integrity issues rise due to factors like multi-tenancy and cloud vulnerabilities. Traditional security measures fall short, emphasizing the need for innovative approaches such as blockchain integration. Recognizing specific threats like confidentiality attacks is crucial for effective security frameworks. Blockchain technology enhances data security, building trust in cloud services for broader industry acceptance.

Key Features of Blockchain that Enhance Data Integrity

Blockchain's decentralized structure improves data integrity by distributing information globally, minimizing risks, enhancing transparency, and ensuring secure data storage through cryptographic methods, collaborating with AI and machine learning for enhanced protection and regulatory compliance.

Implementing Blockchain in Cloud Environments

Incorporating blockchain technology within cloud environments offers a transformative approach to safeguarding data integrity, particularly in multi-tenant architectures where data security remains a significant concern. The immutable nature of blockchain facilitates secure transaction logging, ensuring that any modifications to data are traceable and verifiable, thereby mitigating unauthorized access and tampering risks. Furthermore, the integration of blockchain with existing encryption methods enhances confidentiality, as users can maintain control over their data while leveraging the transparency

Conclusion

Blockchain technology revolutionizes data integrity in cloud settings, addressing ownership and security issues. To empower data subjects and enhance transparency, explicit ownership policies

are crucial. The evolving landscape calls for adaptable frameworks, combining tech advancements and legal changes. Leveraging blockchain's decentralized nature promotes accountability and security, boosting trust and compliance for data integrity and privacy.

Future Implications of Blockchain for Cloud Data Integrity Protection

As organizations rely more on cloud storage, blockchain can play a crucial role in enhancing data integrity. Its decentralized nature provides an immutable ledger for better data verification within cloud environments. By securely documenting each change, blockchain reduces the risks of breaches and unauthorized alterations. Smart contracts help with compliance and auditing, issuing alerts for protocol deviations. Integrating blockchain in cloud setups strengthens security, fosters trust, and meets regulatory data management standards.

References:

- Agrawal, Avish, Bajaj, Raghav, Jaybhaye, Sangita Maheshwar, Phatangare, Sheetal Atul, Savale, Vaishali, Vimal, Aryan. "DStore: Blockchain-Powered Decentralized Cloud Mesh". Auricle Global Society of Education and Research, 2023, https://core.ac.uk/download/588567849.pdf
- Islam, Ashraful. "DATA GOVERNANCE AND COMPLIANCE IN CLOUD-BASED BIG DATA ANALYTICS: A DATABASE-CENTRIC REVIEW". All Academic Research, 2024, https://core.ac.uk/download/624121418.pdf

AI-Driven Cloud Computing Improvements: Synergies between Machine Learning and Generative AI

SINDHU C(23MCA34)

SUBARNA MUKHI A (23MCA36)

Abstract:
AI drastically changed and brought new solutions for cloud computing to elevate utility, scalability, and sustainability. This paper attempts to study the domains of the synergies between ML and generative AI in the cloud. Some of these are applications, benefits, and challenges. Topics include dynamic resource allocation, cost optimization, and the merging of AI-driven technologies to facilitate next-generation cloud systems.

Introduction

Cloud computing has become the backbone of present-day IT infrastructure, with unmatched scalability and efficiency. With the help of modern technologies-born virtualization computing, serverless computing-cloud systems have enabled companies to optimize their operations and innovate.

The hysterical enhancement of automation functionalities, predictive analytics, and resource optimization in cloud computing takes place due to the integration of (ML) Machine Learning and generative (AI) Artificial intelligence.

Machine Learning in cloud computing

ML is a transformative technology that thrives in improving the automation level of processes and providing data-centric intelligence over cloud environments. The applications include:

- Predictive Maintenance: Sensor data examination, allowing anticipation and reduction of downtime for failure.
- Resource Optimization: Dynamic measuring of computational resources to community-based workload demands.
- Customer Experience: Broadening user interactions with improved recommendations or personalized service.

Generative AI Applications

Cloud capabilities have boosted through generative AI by creating new data for many innovative use cases:

- Content Generation: Creating realistic images, videos, or textual data.
- Data Augmentation: Improving training datasets for machine learning models.
- Simulation and Prototyping: Allowing designers and engineers to test designs in a simulated,virtualenvironment.

Benefits of AI-Enhanced Cloud Systems

AI cloud computing offers multiple advantages:

- Cost Efficiency: Showcases elastic scaling and optimal resource usage.
- Innovation: Novel service development opportunities are now opened due to intelligent models.
- Sustainability: Energy consumption is reduced in the name of AI-oriented optimization. This would ultimately result in supporting processes for green initiatives.

Challenges and Considerations
While its integration provides many benefits, there remain a couple of challenges concerning AI in cloud computing.

- Data Privacy-Secure handling of sensitive data.

- Adoption Barriers-Organization resistance and skills gap.

- Ethical Concerns-Dealing with biases and accountability of AI systems.

Future Directions
The pursuit for the next will include the development of autonomous systems, enhancing AI-as-a-service offerings, and collaborations between industry and academia to respond to ethical and technical challenges.

Further building, improving, and advancing these CO2 mitigations requires proper investment

snow.

Conclusion
AI-driven enhancement has redefined cloud computing. With AI and generative AI working in synergy, corporations are enjoying near real-time work and productivity as never before in history, while bringing forth new levels of innovation and sustainability in their processes. There is a need for continued research along this avenue, and the technologies need to be responsibly utilized.

Cloud Computing and Security
The Security Mechanism and Pillars of ERPs on cloud Technology

Sadaf khan CR (23MCA29)

Abstract: Cloud computing is an innovative technology that has transformed organizational data management. It offers cost effective solutions and reliable systems for managing information. However, concerns over security, particularly in the case of Enterprise Resource Planning (ERP) systems, remain significant. This article explores the security mechanisms and foundational pillars that can address these challenges, ensuring the trustworthiness of cloud-based ERP systems.

INTRODUCTION

Cloud computing involves hosting applications, information, and organizational services on remote servers, accessible via the internet. Organizations pay for these services based on usage, making it a flexible and scalable solution. Despite its advantages, cloud computing raises concerns regarding data security, as third party providers often handle sensitive information. This article examines the security vulnerabilities of cloud-based ERP systems and proposes mechanisms to enhance their reliability and confidentiality.

LITERATURE REVIEW

ERP systems have revolutionized business operations by centralizing data and streamlining processes. However, their integration with cloud computing introduces unique challenges, particularly in security. Cloud-based ERP systems offer advantages such as global accessibility, scalability, and cost efficiency. Yet, they also expose organizations to risks like data breaches and compliance issues. Security in cloud computing is hindered by its distributed nature and reliance on third-party providers. Organizations must address these vulnerabilities through robust encryption, access controls, and adherence to legal and regulatory frameworks. Despite these challenges, cloud computing continues to be a transformative technology, offering unprecedented flexibility and efficiency.

RESEARCH METHODOLOGIES AND THEORETICAL FRAMEWORKS

This study employs qualitative research methods to analyse the vulnerabilities of cloud based ERP systems. By examining existing frameworks and security mechanisms, the research highlights the risks and proposes solutions to enhance data protection. The study focuses on the unique challenges posed by cloud computing, such as virtualized environments, compliance issues, and data privacy concerns.

Findings

Cloud computing presents both opportunities and challenges for organizations. Key findings include:

1. Security Vulnerabilities: Cloud systems are prone to data breaches due to inadequate security measures and the involvement of third-party providers.

2. Legal and Regulatory Challenges: The absence of comprehensive legal frameworks complicates data protection and compliance.

3. Advantages of Cloud-Based ERPs:

Despite security concerns, cloud-based ERPs offer scalability, cost efficiency, and global accessibility. To address these challenges, organizations should implement robust encryption

techniques, establish clear legal agreements with cloud providers, and adopt authentication pillars to secure data.

RESULTS OF THE STUDY

Cloud computing has become a transformative technology for organizations, with major providers like Google, Amazon, Microsoft, IBM, and VMware offering diverse services. To secure data in cloud-based ERP systems, organizations should implement encryption for data retrieval and establish legal frameworks for third-party providers. Many cloud providers do not guarantee specific levels of security or privacy, often offering services "as is" without liability. This lack of assurance can hinder organizations from adopting cloud solutions. Clear security measures, transparency, and communication from providers can help reduce perceived risks and build trust. The novelty of cloud computing often leaves customers uncertain about what to expect or demand, relying on the assumption that providers prioritize privacy and security. However, this assumption may not always hold true, creating potential vulnerabilities. Organizations must address technological, behavioural, and perceptual challenges when adopting cloud services. Cloud providers can gain a competitive edge by implementing robust security practices and ensuring clear communication about their protective measures.

CONCLUSION

Cloud computing is one of the modern technology that is useful in many organizations. Cloud computing works on the basis that it provides information in a quick and accessible means within the shortest time possible and form any geographical location. However, the issue of security and data privacy at the cloud-based ERP systems have paused a challenge to many organizations when it comes to adopting this technology. Distributed computing is a multi occupant advantage partaking stage, which allows varied specialist governments to convey software design as administrations and convey equipment as administrations in a practical way. Anyway, alongside these points of interest, putting away a lot of information including fundamental data on the cloud propels profoundly gifted programmers, hence making a major imperative to business information proprietors (Boykin, 2001). Consequently, there is a requirement for the security columns and secretly instrument to be considered and actualized as one of the best arrangements of the urgent issues. Additionally, it innovation with the goal that Legitimate and also ill-conceived associations and substances can be guaranteed to do not accessing information on the cloud through illicit, unprecedented, and semi lawful means (Boykin, 2001). The fears to implement cloud-based ERP systems can be eradicated with the implementation of an authentication pillar to provide secure online services.

QUANTUM COMPUTING IN THE CLOUD:

ANALYZING JOB AND MACHINE CHARACTERSTICS

SANJANA SHARMA M(23MCA30)

AYUSHI DUTT BAGHEL(23MCA06)

ABSTRACT - This paper presents an academic study on resource consumption and job execution trends in quantum cloud systems, focusing on IBM Quantum machines. Over a two-year period, the authors analyse data from over 6,000 jobs, 600,000 quantum circuit executions, and nearly 10 billion shots across 20+ quantum machines. Key areas of analysis include execution times, queuing times, circuit compilation times, machine utilization, and the effects of job and machine characteristics. The study identifies both similarities and differences between quantum and classical HPC cloud systems. Based on the findings, the paper provides recommendations for improving resource and job management in future quantum cloud systems.

INTRODUCTION - Quantum computing, leveraging quantum mechanical phenomena, promises breakthroughs in fields like cryptography, chemistry, and optimization. However, quantum systems are still in the early stages of development, with quantum machines being rare and expensive. Consequently, most researchers access quantum machines via cloud platforms provided by vendors like IBM, Google, and Microsoft.

Trends in Quantum Machines

 Variable Machine Characteristics:

- Quantum machines exhibit differences in topology, qubit strength, calibration quality, and drift, leading to variability in performance.
- For example, T1/T2 coherence times and 2-qubit error rates show significant variation (30-40% and 75%, respectively), indicating a need for better understanding of these characteristics.

 Application Performance:

- An evaluation of the 4-qubit Quantum Fourier Transform (QFT) across IBM quantum machines shows that success probability (POS) can vary significantly, not necessarily correlating with machine size. For example, a smaller 7-qubit machine may outperform a 65-qubit machine in terms of POS, emphasizing the importance of understanding CX-gate characteristics (gate depth, number of gates, and error rates).

 Machine Utilization:

- Smaller quantum machines tend to have higher utilization, while larger machines often face lower utilization due to connectivity constraints and increased circuit depth.
- Machine utilization also varies even within machines of the same size, and decisions are often based on heuristics rather than systematic evaluations, which may waste resources and time.

 Recommendations:

- **CX-gate metrics** should be used at compile time as indicators of application fidelity on a machine, aiding in machine selection.
- To improve **utilization** and **throughput**, vendor-managed resource allocation inspired by HPC systems is recommended.

• **Multi-programming** could enhance machine utilization, particularly on larger machines, by running multiple applications simultaneously while considering system load and application fidelity requirements.

CONCLUSION: In the NISQ era, the growing demand for quantum resources is coupled with their scarcity. To optimize system throughput, quantum machine resources should be efficiently allocated, and clients must adopt effective job deployment strategies to make the most of their allocated time and resources. Understanding the characteristics of quantum jobs and machines is crucial for improving quantum cloud systems. The study, based on an analysis of over 20 IBM Quantum Computers over a two-year period, provides valuable insights that can guide future improvements in resource management and job allocation for quantum cloud systems.