Systemic Analytics

www.sa-journal.org

Syst. Anal. Vol. 3, No. 4 (2025) 232–241.

Paper Type: Original Article

Study on Cloud-Centric IoT Transformation for AC. Manufacturing INC

Ernest Edim*

Department of Environmental Engineering, Faculty of Science, University of Salford, United Kingdom; eedim@edu.salford.ac.uk.

Citation:

Received: 21 June 2025 *Revised: 11 August 2025* *Accepted: 09 September 2025*	Edim, E. (2025). Study on cloud-centric iot transformation for AC. manufacturing inc. *Systemic Analytics, 3*(4), 232-241.

Abstract

Cloud computing is a business approach that is quickly changing our daily lives, and as a result, organisations are more concerned with finding a centralised, affordable solution that offers the highest uptime. This study critically analyses the advantages and disadvantages of implementing a cloud-centric Internet of Things (IoT) transformation for AC. Manufacturing Inc., a mid-sized enterprise in the automotive parts industry. The study aims to expose the integration of cloud-based IoT solutions for real-time monitoring and analytics to streamline operations, improve production efficiency, and enhance real-time decision-making.

Keywords: AC manufacturing INC, Cloud, Cloud-centric, Internet of Things, Transformation.

1 | Introduction

During this paradigm change, AC. Manufacturing Inc. is replacing fragmented legacy systems with a cloud-based Internet of Things (IoT) approach to unify its nationwide operations. Simplified data flow is anticipated by the planned redesign, enabling real-time analytics and monitoring. The company hopes to lead the way in data-driven decision-making, efficiency, and agility throughout all its locations by utilizing platforms such as Google Cloud IoT Core. This will put the company at the forefront of technological advancement in the manufacturing industry. This report delves into the implications of transitioning to a cloud-centric IoT paradigm for AC Manufacturing Inc. It assesses benefits and challenges by considering viewpoints from management, industrial workers, IT personnel, and vendors. Specific areas to be explored include the advantages of cloud-based services, security and compliance, cloud service structures, virtualization in servers and networks, and the complexities of migration. Real-world examples and practical experiences are used to analyse the nuances of setting up a cloud environment. The report compares Cloud-based and local IT resources. It serves as a valuable guide for AC Manufacturing Inc. to make informed decisions and emerge as an innovation leader in the competitive automotive components sector.

Corresponding Author: eedim@edu.salford.ac.uk

https://doi.org/10.31181/sa34202559

2 | Opportunities and Challenges of Cloud Migration

Cloud migration transfers an organisation's data, applications, and IT processes to cloud-based infrastructure. It presents many opportunities and challenges. Understanding and handling these factors is critical for organisations trying to reap the benefits of cloud computing while limiting potential hazards.

2.1 | Opportunities of Migrating IT Resources to Cloud Computing

Cloud computing is a business approach that is quickly changing our daily lives. These days, organisations are more concerned with finding a centralised, affordable solution that offers the highest uptime [1]. Anybody using the internet is involved in cloud computing, whether they realize it or not [2]. An increasing number of mobile users can now easily store their mobile data on cloud computing, eliminating the need for manual data storage [3]. The benefits of cloud computing include its ability to provide a company with numerous services, including scalability, dependability, flexibility, and work-from-anywhere capabilities [4]. Data migration to the Cloud is affordable, considering the costs associated with on-premises hardware, software, employees, downtime, and depreciation [1], [5]. Outsourcing their primary infrastructure services to cloud service providers while focusing on their core business is one of the main advantages for organisations. Another benefit is the low energy cost. Because cloud computing uses less energy and has more environmentally friendly features than on-premises systems with fewer physical materials being used. Any organisation that wishes to remain competitive in today's economic environment must address the integrity and reliability of crucial data, which is something that cloud vendors must also do [6]. The responsibility of cloud vendors is to guarantee the security of their infrastructure and the protection of their client's data and applications. Using encryption techniques, cloud service providers offer a high-level security protocol to confirm data protection [7]. Cloud providers' intricate data centres are constructed using layered security techniques, such as key management, data encryption, stringent access controls, and adherence to frequent security audits [8].The availability of these secured cloud vendors makes migration to Cloud computing a big opportunity to be explored by the company. Most service providers enable enterprises to expand their resources to meet changing business needs by offering scalable IT resources [9]. It may be necessary for specific customers to adjust their IT resources quickly. This will allow for business growth to be supported without incurring costly changes to the current system infrastructure [10]. Managing resource demand in traditional computing systems can pose challenges, but the utilisation of cloud resources can provide a viable solution for handling increasing workloads in any application [1].

2.2 | Challenges of Migrating IT Resources to Cloud Computing

The process of transferring data from a legacy system to the Cloud for data management and migration poses important study issues that should not be underestimated. It is not easy for an organisation to select a good cloud provider, even after performing a SWOT (Strength, weakness, opportunities, and threats) analysis. The three prominent entities in the cloud industry, namely Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure, consistently strive to differentiate themselves from each other. Because of this, businesses must question cloud providers about their data migration tools to move data while taking vendor lock-in and software portability (The capacity to move software from one computer or system to another) into account. Change management is essential for projects like these. Costs may increase if staff members need to be trained on a new software platform and system. Furthermore, how staff members behave when adjusting to the new system presents another difficulty, i.e., change management must be done correctly and promptly. Hence, accessing cloud content may pose a challenge and operational downtime. Hardware or software failure is not always the cause of a system failure; effective IT practices and infrastructure procedures are the foundation of digital transformation [11], [12]. A plan for supporting the change must be created, implemented, and monitored during data and process migration. Many organisations worldwide are integrating cloud computing as a fundamental element of their technology strategy [13]. Despite the overwhelming momentum towards cloud adoption, cost-benefit analysis models that show the business impact remain a significant risk factor [14]. Before moving to the cloud, it can be difficult to redesign your

current IT infrastructure (Server, network, and storage) to meet the requirements. Pay-as-you-go cloud providers impose variable costs on their users based on the number of transactions they process and their number of users [15]. Businesses are hesitant to pay more for management, additional bandwidth costs, and system acquisitions. Cloud market leaders have been touting their most recent data security model. Still, the NSA snooping scandal makes people question and reconsider storing all sensitive and vital data in the Cloud. This lack of trust impacts all significant stakeholders, including governments, corporations, and individual citizens. Data security breaches, lack of service quality, such as 24/7 support from vendors, and poor data backup and recovery are among users' fears of migration to cloud computing. Since cloud-based data is easily accessible from any location, personal and business data may be compromised by hacking or data breaches brought on by weak password security. The organisations had complete control and authority over the local hosting of their data. Since hackers frequently target large data centres, they might feel more exposed when moving to the Cloud.

3 | Security, Compliance, and Risks of Migrating IT Resources to Cloud Computing

3.1 | Security

Customers rank cloud security as one of the biggest challenges. Utilizing the service necessitates in-depth investigation to comprehend the threat's potential and its effects on enterprises. According to a thorough survey by Ramachandra et al. [16], demand for cloud-based security is trending upward, and costs are rising to keep up with modern demands. For instance, the analysis revealed that from 2011 to 2015, the percentage of cloud-based security pending increased by 10% annually [16]. The following enumerates the significant threats and issues of today's cloud security. There is an increased need for in-depth research on cloud security to provide workable solutions for the problems [17]. Higher privileges should be used to enable access to data on cloud tools [18]. This will strengthen cloud security. Critical steps are outlined by the National Institute of Standards and Technology (NIST) to raise the bar for cloud computing and cloud service access while maintaining the highest level of data security [19]. As a result, the report highlights how vital cloud security is and that it should be considered when using cloud computing services.

3.2 | Compliance

It can be challenging to follow industry-specific laws and compliance requirements. Cloud service providers must provide guarantees and resources to assist businesses in meeting these needs. Data must be stored within specified geographic areas according to specific regulations. It can be challenging to ensure that jurisdictional concerns are addressed, and data residency requirements are met. Cloud environments need robust audit trails and monitoring systems to meet compliance requirements [20]. It is essential to guarantee visibility into user actions and system modifications.

3.3 | Risk

Risks can arise from relying too much on one cloud service provider. A business may encounter difficulties with a smooth migration of data and applications if it chooses to switch providers. Trying to migrate to the Cloud without a clear, comprehensive plan is one of the most significant risks involved in the process [21]. An organisation must choose which cloud platform or platforms to use, how to distribute IT assets, and how to deploy applications when moving to the Cloud. A cloud migration process's expense, time, and complexity can all rise if these and other crucial decisions are not made in advance. Making incorrect choices can pose serious security risks, such as processing or storing private data in a public cloud environment [22].

4 | Structure, Services, and Deployment Models

The deployment model and service selection primarily determine a cloud computing platform's degree of vulnerability. According to [23], three delivery models and three deployment models are regarded as industry standards. Security implications are distinct for each of these three deployment and delivery models. A brief explanation of each of these models' security implications is provided in the subsections that follow:

4.1 | Cloud Service Models

The industry has adopted three cloud service models, which were suggested by [23–25]: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). This is illustrated in *Table 1*.

Table 1. Cloud service types and their characteristics.

Service Type	Benefits	Challenges	Risks
Infrastructure as a Service (IaaS)	The fundamental components of cloud computing, such as servers, virtualizations, network infrastructure, and network-accessible storage that enables users to run any software, are provided by infrastructure as a Service (IaaS).	Heavy reliance on external vendors. Security breach issues [26].	Both cloud service providers and cloud users bear equal responsibility for security measures. There are layers and segregations of risk in this model. The model of shared risk is also present.
Platform as a Service (PaaS)	Platform-as-a-Service (PaaS) is a popular option for enterprises looking for streamlined and effective application development and deployment because of its advantages, which include streamlined development environments, integrated services, cost-effectiveness, increased productivity, rapid deployment, and scalability.	The possibility of vendor lock-in is a significant obstacle related to Platform as a Service (PaaS). Platform as a Service (PaaS) providers provide a particular set of tools, development frameworks, and services that may be exclusive to their Platform or proprietary. Therefore, moving to a different PaaS provider or developing the application internally may be difficult once a company develops and implements applications utilizing these platform-specific features.	Data security and privacy compromise is one of the major risks connected with Platform as a Service (PaaS). Sensitive data is frequently processed and stored within PaaS environments, which organisations utilise to develop, deploy, and manage applications. Unauthorized access, data breaches, and data loss can result from several factors, including insufficient access controls, flaws in the PaaS infrastructure, and incorrect configurations.
Software as a Service (SaaS)	Numerous businesses find the software as a Service (SaaS) model appealing due to its multiple advantages, including automated updates, scalability, accessibility, cost efficiency, and the freedom to concentrate on core competencies.	The tricky part is ensuring the cloud provider has robust security measures, such as encryption, access controls, and frequent security audits. Organisations must also assess the provider's data handling procedures, adherence to data protection laws, and response mechanisms in case of a security breach. One of the main challenges with the SaaS model is still finding the right balance between convenience and data security.	Reliance on the dependability and stability of the software as a Service (SaaS) provider is a major risk involved with SaaS. A provider's downtime, service interruptions, or outages immediately affect users' access to the SaaS application. During these times, businesses that rely significantly on essential SaaS apps may experience operational difficulties and a decline in productivity.

4.2|Cloud Deployment Models

Cloud deployment models can be broadly classified into three types [24], [25]. They are Hybrid, Public, and Private. This is shown in *Table 2*.

Table 2. Cloud deployment models and their characteristics.

Deployment Type	Benefits	Challenges	Risks
Private Cloud	The private cloud deployment model provides improved security, customization, intranet functionality, predictable billing, scalability, and compliance adherence. Because of these features, it is a desirable alternative for companies with requirements and a focus on security and control.	Security challenges include the high expense of implementation and management, the need for specialized knowledge, and vulnerability management. Cost and return on investment are important considerations in this deployment model. Security implementation is typically predicated on risk assessment, meaning the security cover is incomplete.	The possibly high implementation and upkeep costs are some of the associated risks. A significantinitial/capital investment in hardware, software, and qualified staff is necessary to establish and upkeep a private cloud infrastructure. The company is responsible for continuous upkeep, modifications, and guaranteeing the scalability of the infrastructure, which may result in supplementary expenses in the future.
Public Cloud	The public cloud model is an appealing choice for various industries. Itis used due to its advantages: scalability, cost-effectiveness, global accessibility, less maintenance required, rapid deployment, elasticity, and access to advanced services.	The increased security and privacy issues of sharing resources and infrastructure with numerous users present a significant obstacle. Public clouds' multi-tenant architecture increases the possibility of data breaches, unwanted access, and the possible exposure of private data.	The potential compromise of data privacy and regulatory compliance is a major risk associated with public clouds. Concerns regarding data isolation and the possibility of unwanted access arise when sensitive data is stored in a multi-tenant setting. Businesses operating in highly regulated sectors or areas face difficulty adhering to industry-specific rules, data protection laws, and other legal obligations.
Hybrid Cloud	Although there is a risk that data privacy and regulatory compliance will be compromised, there are advantages to using public clouds strategically, including adherence to international compliance standards, improved security measures, access to knowledge and resources, effective compliance management, and data residency options.	The reliance on the cloud service provider is one of the main issues with public clouds. Businesses give up some control over the provider regarding data management, service configurations, and infrastructure. This reliance may present a problem if businesses cannotoptimize or customize services to meet their unique requirements.	The reliance on network connectivity and possible dependability problems poses a serious risk to public clouds. Any hiccups or slowdowns in internet connectivity can affect the availability and functionality of cloud-based applications, as public clouds depend on it for users to access resources and services.

5 | Concept of Virtualization in the Context of Servers, Storage, and Network Systems

Virtualization in the context of cloud computing goes beyond separate elements such as servers, storage, and networks. It includes a whole strategy in which these components are dynamically assigned, aggregated, and abstracted according to demand [26]. The foundation of cloud services is created by combining virtualization for servers, storage, and networks, resulting in a comprehensive and adaptable environment. Network virtualization is essential to building a versatile and flexible networking infrastructure in the Cloud [27]. Several virtual networks can be built on top of a single physical network through the abstraction of network resources. This separation improves security, isolation, and the effective use of network resources.

A fundamental server virtualization featuredivides a physical server into several virtual servers, each running separately. This makes it possible to allocate computational resources efficiently and optimize hardware use [28]. Users can quickly adjust to changing workload requirements and scale up or down by provisioning or de-provisioning virtual machines. Comparably, abstracting physical storage resources into a single, controllable pool is the goal of storage virtualization. Thanks to this abstraction, users can dynamically allocate or de-allocate storage based on their demands, allowing for the efficient use of available capacity. It makes data management more accessible, increases flexibility, and lowers costs. Cloud service providers attain elasticity and scalability by implementing virtualization throughout various areas [26]. Users no longer have to worry about the complexities of the physical infrastructure when adjusting resource levels to meet demand variations. The ability of cloud service providers to optimize resource utilization, improve productivity, and reduce operating expenses is made possible by this dynamic resource allocation. Thus, the cloud computing paradigm's foundation is virtualization, which offers flexible, scalable, and affordable solutions to satisfy various user needs.

6 | Strategies for Migration and Business Application Benefits

Selecting a migration strategy is a strategic move that needs to be carefully considered in relation to the unique aims and objectives of the company. When choosing a migration strategy and utilizing cloud benefits, it's critical for businesses to carefully assess their specific needs and goals to make sure the chosen approach seamlessly aligns with their overall goals. This strategic alignment maximizes the benefits to overall business performance and helps to ensure that cloud resources are used effectively. Cost savings, scalability, global accessibility, security, and disaster recovery are just a few advantages Cloud computing offers businesses to improve their operations [29]. In addition to the benefits described above, cloud computing provides enterprises with increased flexibility and agility. Cloud platforms enable rapid resource deployment, allowing firms to quickly adjust to changing market conditions or fluctuations in demand [30].

Moreover, cloud services frequently include built-in collaboration features, which promote better communication and coordination among employees, even in geographically distant teams. Furthermore, the scalability of cloud solutions guarantees that companies may effortlessly expand or contract their operations per their present requirements. In addition to optimizing resource utilization, this eliminates the need for large infrastructure investments, which can result in significant cost savings. The ability to innovate and experiment is another crucial benefit. Cloud environments offer an ideal platform for testing and creating new services, features, or applications without requiring significant upfront costs [31]. This encourages an innovative culture within the company, which drives ongoing development and technology adaptation [32].Additionally, cloud-based systems frequently provide strong security and compliance capabilities. This is especially important given the state of the digital world today when privacy and data protection are top priorities. Cloud providers usually invest significantly in security processes so companies can confidently function in a safe and legal environment. Finally, operating remotely is possible because cloud services are accessible from almost any location with an internet connection [23]. This has grown in significance, particularly given the prevalence of

flexible work schedules in today's corporate environment. By utilizing cloud technologies, staff members may participate in business activities from anywhere in the world, collaborate easily, and access data remotely.

7 | Issues in Setting up and Configuring Cloud Environments and Virtual Machines

7.1 | Practical Experience

Critical issues affecting IT infrastructure's effectiveness, security, and performance must be addressed when setting up and configuring cloud environments and virtual machines. I attended a workshop where we worked with a popular cloud service provider to configure a cloud environment for a web application. An increase in user demand brought about performance problems due to difficulties in effectively allocating resources. A clear plan for managing different workloads was absent from the setup. This emphasized the significance of strategizing for scalability and resource provisioning to prevent poor performance or outages during periods of high demand. To maximize resource utilization, the workshop highlighted the importance of dynamic scaling features like auto-scaling groups. It emphasized the importance of thoroughly grasping application usage patterns and utilizing cloud-native features to enable automatic scaling. Identifying potential scalability bottlenecks and ensuring a responsive and resilient cloud environment required early implementation of capacity planning and load testing during the setup process.

7.2 | Criteria for Comparison

Table 3 shows the comparison between the deployment of cloud resources and locally-based IT resources. This comparison highly the features of each model, aiding better understanding for easy decision making by the management.

Table 3. Comparison between cloud solution and locally based IT infrastructure.

Critical Issues	Cloud Environment	Locally Based IT Resources
Resource Provisioning	Dynamic scaling based on demand.	Limited scalability and upfront investment in hardware.
Cost Management	Pay-as-you-go model, potential cost savings.	Upfront costs for hardware and maintenance.
Flexibility and Agility	Rapid deployment and flexible resource allocation.	Limited flexibility and time-consuming setup.
Security Concerns	Data security is in the hands of the provider.	Direct control but may lack advanced security.
Network Connectivity	Dependence on internet connectivity.	Intranet-based, potentially more reliable.
Configuration Complexity	Learning curve for cloud-specific configurations.	Familiarity with on-premises systems.
Data Transfer and Latency	The internet impacts data transfer speed.	Faster data transfer within on-premises infrastructure.
Scalability Challenges	Ensures seamless scalability without disruptions.	Limited scalability and potential downtime during expansion.

8 | Conclusion

This report has explored the opportunities, benefits, and challenges in moving the IT operations of AC Manufacturing Ltd from locally based IT resources to a cloud environment. The security, compliance, and risk associated with this migration have been discussed. The structure, services, and deployment models such as IaaS, PaaS, SaaS, public cloud, private cloud, and hybrid cloud have been discussed with highlights focused on the benefits, challenges, and risk as it relates to the IT infrastructure upgrading intentions of the company. It is anticipated that this migration will greatly improve efficiencies in operations and facilitate rapid decision-making as all operations are connected to the cloud environment. Finally, a comparison between the cloud environment and locally base IT infrastructure was highlighted to give a robust understanding of the anticipated move.

Author Contributions

EE: Conceptualization, Writing, Editing, Resources, Visualization. The author read and approved the manuscript.

Data Availability

Not applicable.

Funding

This research received no external funding.

Acknowledgement

The authors appreciate the editor and reviewers for adding valuable input to the manuscript.

References

[1] Iqbal, A., & Colomo-Palacios, R. (2019). Key opportunities and challenges of data migration in cloud: results from a multivocal literature review. *Procedia computer science*, *164*, 48–55. https://doi.org/10.1016/j.procs.2019.12.153

[2] Adeniran, A. O., Folorunso Segun, S., Babawole, F. O., & Victoria, M. O. (2024). Adoption of fourth industrial revolution technologies in the construction sector: Evidence from previous studies. *International journal of innovation in engineering*, *4*(3), 1–18. https://doi.org/10.59615/ijie.4.3.1

[3] Goudarzi, M., Ilager, Sh., & Buyya, R. (2024). Cloud computing and internet of things: recent trends and directions. *In new frontiers in cloud computing and internet of things*. Springer. https://link.springer.com/chapter/10.1007/978-3-031-05528-7_1

[4] Stantchev, V., Colomo-Palacios, R., & Niedermayer, M. (2014). Cloud computing based systems for healthcare. *The scientific world journal*, *2014*, 692619. https://doi.org/10.1155/2014/692619

[5] Ilugbami, O. J., Tolu, O. O., Abdulmateen, G. A., & Odeyinka, Y. V. (2025). Cybercrime and cyber-security in Nigeria. *Management analytics and social insights*, *2*(3), 230_244. https://doi.org/10.22105/masi.v2i3.77

[6] Singh, A. (2013). *Is big data the new black gold?* https://just-tech.ssrc.org/citation/is-big-data-the-new-black-gold/

[7] Gholami, M. F., Daneshgar, F., Low, G., & Beydoun, G. (2016). Cloud migration process—a survey, evaluation framework, and open challenges. *Journal of systems and software*, *120*, 31–69. https://doi.org/10.1016/j.jss.2016.06.068

[8] Misra, S. C., & Doneria, K. (2018). Application of cloud computing in financial services: An agent-oriented modelling approach. *Journal of modelling in management*, *13*(4), 994–1006. https://doi.org/10.1108/JM2-12-2017-0131

[9] Reza Bazi, H., Hassanzadeh, A., & Moeini, A. (2017). A comprehensive framework for cloud computing migration using Meta-synthesis approach. *Journal of systems and software*, *128*, 87–105. https://doi.org/10.1016/j.jss.2017.02.049

[10] Mishra, N., & Kumar, N. (2015). Load balancing techniques: Need, objectives and major challenges in cloud computing-a systematic review. *International journal of computer applications*, *131*(18), 11–19. http://dx.doi.org/10.5120/ijca2015907523

[11] Adeniran, A. O. (2017). Idea of smart development in the fourth industrial revolution emphasis on smart road. *SF j. telecommun*, *1*, 1–6. https://d1wqtxts1xzle7.cloudfront.net/59812915/2017

[12] Cardoso, A., Moreira, F., & Simões, P. (2014). A survey of cloud computing migration issues and frameworks. In *New perspectives in information systems and technologies, volume 1* (pp. 161–170). Springer. https://doi.org/10.1007/978-3-319-05951-8_16

[13] Khan, N., & Al-Yasiri, A. (2016). Framework for cloud computing adoption: a road map for Smes to cloud migration. *ArXiv preprint arxiv:1601.01608*, 1_15. https://doi.org/10.48550/arXiv.1601.01608

[14] Litchfield, A., & Althouse, J. (2014). A systematic review of cloud computing, big data and databases on the cloud. https://www.researchgate.net/profile/Alan-Litchfield/publication/289153623

[15] Rajkumar, M. N., Venkatesakumar, V., Mahadevan, M. T., & Chatrapathi, M. C. (2014). Security measures in cloud computing an extensive assessment. https://just-tech.ssrc.org/citation/is-big-data

[16] Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. *Procedia computer science*, *110*, 465–472. https://doi.org/10.1016/j.procs.2017.06.124

[17] Alsaadi, E. M. T. A., Fayadh, S. M., & Alabaichi, A. (2020). *A review on security challenges and approaches in the cloud computing* [presentation]. AIP conference proceedings (Vol. 2290, p. 40022). https://doi.org/10.1063/5.0027460

[18] Singh, V., & Pandey, S. K. (2019). Revisiting cloud security threats: Elevation of privilege. *International journal of advanced studies of scientific research*, *4*(2), 499-507. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331932

[19] Jansen, W. A., Grance, T., & others. (2011). *Guidelines on security and privacy in public cloud computing*. [Thesis]. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf

[20] Duncan, B., Whittington, M., & others. (2016). Cloud cyber-security: Empowering the audit trail. *International journal on advances in security*, *9*(3). 169-183. https://abdn.elsevierpure.com/en/publications/cloud-cyber-security-empowering-the-audit-trail

[21] Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A risk management framework for cloud migration decision support. *Journal of risk and financial management*, *10*(2), 1-24. https://doi.org/10.3390/jrfm10020010

[22] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

[23] Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., … & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. *Automation in construction*, *122*, 103_441. https://doi.org/10.1016/j.autcon.2020.103441

[24] Patel, H. B., & Kansara, N. (2021). Cloud computing deployment models: a comparative study. *International journal of innovative research in computer science & technology (IJIRCST)*, 315_322. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3832832

[25] Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. C. (2022). Adoption of cloud computing as innovation in the organization. *International journal of engineering business management*, *14*, 18479790221093990. https://doi.org/10.1177/18479790221093992

[26] Dawoud, W., Takouna, I., & Meinel, C. (2010). *Infrastructure as a service security: challenges and solutions* [presentation]. 2010 the 7th international conference on informatics and systems (INFOS) (pp. 1–8). https://ieeexplore.ieee.org/abstract/document/5461732

[27] Arogundade, O. R., & Palla, K. (2023). Virtualization revolution: transforming cloud computing with scalability and agility. *IARJSET*, 1588_2394. https://doi.org/10.17148/IARJSET.2023.106104

[28] Duan, Q. (2021). Intelligent and autonomous management in cloud-native future networks—A survey on related standards from an architectural perspective. *Future internet*, *13*(2), 42. https://doi.org/10.3390/fi13020042

[29] Co, H. T. (2023). *Cloud Computing Technology*. Springer. https://doi.org/10.1007/978-981-19-3026-3

[30] Xue, C. T. S., & Xin, F. T. W. (2016). Benefits and challenges of the adoption of cloud computing in business. *International journal on cloud computing: Services and architecture*, *6*(6), 1–15. https://doi.org/10.5121/ijccsa.2016.6601

[31] Besim, R., & Sharma, B. P. (2023). *The impact of cloud computing on marketing and management*. https://www.researchgate.net/profile/Bishnu-Sharma-13/publication/368825017

[32] Attaran, M., & Woods, J. (2019). Cloud computing technology: Improving small business performance using the Internet. *Journal of small business & entrepreneurship*, *31*(6), 495–519. https://doi.org/10.1080/08276331.2018.1466850

[33] Abell, T., Husar, A., & May-Ann, L. (2021). Cloud computing as a key enabler for tech start-ups across asia and the pacific. *ASIAN development bank*, 1_38. http://dx.doi.org/10.22617/WPS210253-2