Deployment Models of Cloud Computing: Public, Private, Hybrid, and Community Clouds

Chhaya Porwal[1], Sonu Airen[2], Puja Gupta[2*]

[1]Data Specialist, IBM India Pvt Ltd
[2]Assistant Professor, Shri G.S. Institute of Technology & Science, Indore, M.P. India

Abstract

Cloud computing has been transforming the way organisations store, process, and manage data. Because of the different deployment models, organisations can select any cloud service that fits their needs. This paper will explore and compare four major types of cloud deployment models that include Public, Private, Hybrid, and Community clouds. We will study and analyse the literature review with respect to each of these models to examine their advantages and limitations as well as determine their use cases. The study will strive to explain the specific characteristics of models and suggest which of the models of deployment best satisfies organisational requirements in terms of scaling, security, and cost-effectiveness.

Keywords: Cloud computing, Public cloud, Private cloud, Hybrid cloud, Community cloud, Deployment models

I. INTRODUCTION

Cloud computing is one of the latest technological revolutions to come forth within the current digital age, resulting in a paradigm shift for businesses and governments as well as for ordinary people related to accessing and managing computing resources. Shared infrastructure provides access to users who then utilise colossal computational power, enormous storage capacity, and networking capabilities with reduced costs and optimised efficiency. The digital transformation is spreading to organisations throughout the world, for which cloud computing provides flexible and scalable services to cater to data and processing requirements that are constantly growing. With the adoption of cloud computing increasing by leaps and bounds, types of deployment models, which include public, private, hybrid, and community clouds, are essential to choose the right architecture according to the business needs and security issues as well as for operational efficiency.

Cloud computing primarily guarantees the availability of computing services on-demand over the internet, doing away with the need for organisations to invest heavily in local hardware and software infrastructure. One of the most widely accepted definitions of cloud computing has been provided by the National Institute of Standards and Technology: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" [1]. The other side of this coin of great benefit is selecting an appropriate deployment model so that the ultimate focus of these benefits and extra considerations about security, compliance, and tailoring are met.

The three types of deployment models for cloud computing mainly vary based on control, access, and targeted user base. Third-party service providers are managing public clouds with the greatest advantages-from scalability and cost-effectiveness that often drive companies and individuals to adopt this model-the greatest deployment model adopted so far. These clouds are accessible to the public over the internet, providing an attribute of pay-per-use for companies and users. Major companies in this market are tech

giants Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, which have an enormous selection of services ranging from virtual machines to AI-driven analytics. However, public clouds also carry along these benefits worries over data security and privacy as well as issues of regulatory compliance for organisations working in industries that are highly regulated, such as health and finance [3][4].

Private clouds are specifically customised environments that exclusively support a single organisation. They could be on-premises or at any third-party provider and provide better security, control, and personalization. Private clouds are isolated from public networks, meaning businesses can meet the stringent regulatory requirements and ensure full control over data [10]. In recent times, for example, the health sector has implemented many private cloud models to comply with the data protection acts of various countries, such as HIPAA in the United States [6]. Private clouds may ensure better security and control but are usually expensive and demand more high-powered IT for its management.

Hybrid clouds will enable organisations to benefit from both public and private clouds; that is, they can keep sensitive workloads in their private cloud and ensure scalability in other aspects by using public cloud resources for relatively less important tasks. The model will optimise the business infrastructure since critical applications stay on-premises, while others can be offloaded in the public cloud when the need arises. Hybrid cloud deployments are flexible and have been offering companies the best of both worlds: cost efficiency, scalability, and security, that is why hybrid cloud deployments become an attractive option for businesses having dynamic or unpredictable workloads [24]. For example, a firm could make use of a private cloud for the storage of its sensitive customer data and a public cloud to have additional processing power during peak periods of traffic.

Though less common, community clouds provide a highly specific model of deployment suited to a particular type of organisation with common goals or regulatory requirements. These are typically controlled and operated by organisations themselves or by a third-party supplier for the account of the group. Community clouds are therefore often encountered in healthcare and educational establishments or government organisations where there is a blend of various organisations, each having common infrastructures, yet meeting the stringent standards of compliance. Community cloud is used by universities in the higher education departments that unite to pool together the resources for researchers and other academic approaches as a cost-effective approach to collaboration [13].

Choice of cloud deployment model An organisation selects from one of three generic deployment models based on the size and type of organisations, stringent regulatory requirements, and budget. Public clouds are ideal for businesses that anticipate scalability and a minimum involvement with infrastructure management. Private clouds are applicable to organisations that require strict security and compliance requirements. Hybrid clouds are a middle ground that facilitate the ability to balance workloads across both public and private environments. The community clouds serve a niche market where organisations come together to share resources to meet common objectives.

Inter-domain boundaries will continue to dissolve as innovation tends to blur the distinction between deployment models; multi-cloud strategies are already gaining acceptance. A multi-cloud approach would enable an organisation to take advantage of several cloud services from different providers with optimised performance, avoid vendor lock-in, and improve resilience. However, these bring with them new challenges related to the management of security, interoperability, and compliance with different cloud-based

environments. The future of cloud computing will also witness greater involvement of these deployment models, enticed by ever-increasing demands for greater flexibility, security, and innovation.

II. LITERATURE REVIEW

Cloud computing, as a technological paradigm, has picked pace tremendously across industries in order to revolutionise the manner through which organisations managed, stored, and processed their data. Most of the previous studies carried out have been aimed at focusing on the different deployment models of cloud computing public, private, hybrid, and community clouds-aqua offer different benefits and difficulties at times depending on the type of usage. This literature review section delves deeper into how these models of deployment have been discussed in the literature with special emphasis on the factors that influence adoption, security considerations, and sector-specific use cases.

Public Cloud Deployment

Public clouds have led the market of cloud computing because they are offering a cost-effective, scalable, and accessible solution. Quite a few of the researchers have pointed out that public cloud platforms are all-inclusive. These platforms, with the involvement of third-party vendors, provide businesses with access to or scale of the resources on-demand and do not need to invest in or maintain physical infrastructure. Public cloud services are offered via the internet for extending wide access to various types of users [1]. These vary from individual customers to large organisations. The leaders in these services are AWS, Google Cloud, and Microsoft Azure, and they offer IaaS, PaaS, and SaaS models.

The adoption of public cloud services is not trouble-free. Data security and privacy issues are the primary reasons for their more limited adoption in sensitive industries such as health and finance and even though Malaysia's healthcare industries increasingly embrace cloud services, limitations on data sovereignty, regulatory compliance, and confidential information of patients hinder wider adoption [3][4]. Thirdly, breaches in a public cloud setting may have profound implications; therefore, organisations implement strict security protocols and encryption techniques to secure sensitive information [2].

The above scenario is in sharp contrast to the fact that public cloud services are highly popular today, owing to the uptake of these services by SMEs and start-ups. Because of their flexibility and pay-per-use model, public clouds are now an equally suitable option for businesses scaling up their operations with minimum overhead when it comes to managing complicated IT infrastructures [24]. Research further provides that public clouds are an appropriate environment for enterprises that want applications and services to be deployed rapidly to stay competitive in dynamic markets [10].

Private Cloud Deployment

Private clouds offer a more secure and controlled environment, mainly for organisations that have specific regulatory and compliance requirements. They are mostly hosted on premises or by a third-party provider but are dedicated to a single organisation. Private clouds ensure better data security and control, which is crucial when sectors involve sensitive information [8]. For example, with private cloud infrastructure, health organisations assure confidentiality to the patients and thus ensure compliance with data protection laws, for example, Health Insurance Portability and Accountability Act (HIPAA) [4].

The biggest advantage of private cloud deployment is that it ensures the same level of scalability and flexibility as with public clouds but provides great customizability and control. The organisations can tailor their cloud environments according to business-specific requirements. In this manner, the sensitive data is kept behind corporate firewalls. Yet again, this better security and control are achieved at a price. Private clouds are relatively costlier to establish and sustain; therefore, they require significant IT resources and

investments in terms of infrastructure [26]. Still, the security benefits make private clouds an attractive choice of any enterprise in highly regulated industries.

The Malaysian healthcare sector showed a significant preference for private cloud solutions because of the confidential nature of the medical records and strict policies that govern data handling [6]. Also, eHealth systems all around the developing countries prefer private clouds in order to keep proper control over critical patient data [5]. Although the financial and technical constraints associated with private cloud usage do remain a concern for many organisations, particularly the smaller ones, that possess very limited IT budgets, hybrid cloud deployment will remain the fastest-growing model in years to come.

Hybrid Cloud Deployment

Hybrid cloud models have been identified as a solution that takes the best of public and private clouds. Hybrid models allow firms to keep all their critical workloads or applications within private clouds but use public clouds for tasks that are not so sensitive. This increases flexibility, cost savings, and scalability. It is specifically helpful for those firms with fluctuating workloads as well as organisations where efficiency in cost has to be balanced with security and compliance imperatives.

Therefore, organisations can make apt use of resources and achieve greater operational efficiency with greater ease by flawlessly switching between the public and private clouds. Hybrid clouds can help higher education institutions utilise public cloud infrastructure in cases where sensitive research projects require involving student data maintained on servers of private clouds [13]. This hybrid approach gives stronger security and at the same time reduces the cost, and hence the hybrid cloud scenario is attractive for organisations who have dynamic workloads.

Other than these benefits of cost and flexibility, hybrid clouds possess stronger capabilities on disaster recovery and business continuity. Organisations can implement public clouds as backup environments to guarantee that the services will remain in operations during failure or disaster [17]. This is significant, given that for industries which include banking and healthcare, downtime gives rise to severe financial and operational implications. However, hybrid models of clouds make matters more complicated concerning management and security on account of the necessity to ensure alignment between the public and private environments concerning the community cloud deployment [16].

Community Cloud Deployment

Community clouds, although not as popular, are meant specifically to be used by organisations that have a common goal, regulation, or security in mind. These clouds are typically developed and operated by a consortium of organisations, such as government agencies, colleges, and universities or hospital systems, that share common infrastructure while still maintaining complete control over their own information [20]. A clear benefit of community clouds is the ability to share resources among organisations with related needs, along with the costs that are associated with managing different infrastructures for separate IT systems.

In education, universities in Malaysia have adopted community cloud models for increasing mobile learning and inter-institutional collaboration [15]. Such a cloud environment provides a secure space for collaboration and research that improves the delivery of services while reducing costs of operation. Governments also employed a community cloud to promote information sharing and interagency collaboration, which thereby made them offer e-government services in an efficient manner [17].

Although community clouds offer some benefits, few companies have embraced them as a result of governance and ownership of data as well as security issues. There is a common agreement on aspects relating to resources management, who can access shared data, and how security is guaranteed across the cloud environment [18]. However, as cloud computing remains an evolving entity, community clouds may be applicable for organisations with specific objectives as well as compliance requirements.

III. METHODOLOGY

Methodology of "Deployment Models of Cloud Computing: Public, Private, Hybrid, and Community Clouds.". This research utilises the mixed methods design that would apply both the quantitative and the qualitative approach in order to gain a total comprehension of the problem under study. The research methodology is divided into four crucial subsections, namely: Research Design, Data Collection, Data Analysis and Tools/Software. In detail, procedures, techniques, and strategies followed during the conduct of this study in justification of how to make the outcome valid and reliable, are explained underneath each sub-section.

1. Research Design

This research is applied under a mixed-method approach since it falls under both the quantitative and qualitative data. It is because it offers a deeper understanding of cloud computing deployment models, with both numerical data and insightful qualitative understandings.

After all, deployment models of cloud computing mix the measurable technical and operational dimensions: cost efficiency, scalability, and performance metrics; with qualitative ones-user satisfaction, security perceptions, organisational needs. A mixed-method approach would be ideal because it makes it possible to discuss these two dimensions. This information would help calculate how efficient it was with security as well as allow a comparison of the rates of adoption for each of the respective deployment models. Qualitative information on the other hand would help delve deeper into understanding and exploring organisational experiences and challenges regarding such models.

The study started with the quantitative phase that gathered data regarding number-based information from the relevant surveys and case studies of adoption rates, cost savings, and performance benchmarks on both the public, private, hybrid, and community clouds. Further, the research utilised the qualitative phase using interviews carried by IT professionals, cloud service providers, and end-users to provide the view of these different models of cloud computing.

1.2. Research Design Purpose

This design basically tries to answer two types of research questions.

1. Descriptive and comparative type, focuses on the description of the features and comparison of the effectiveness of the differences of the cloud deployment models in terms of scalability, cost, and security.
2. Exploratory and interpretive type: This concerns the underlying factors informing the adoption of these models and challenges and organisations face while making the right choice of a deployment model.

The research design was structured in such a manner as to be amenable to both descriptive statistical analysis and thematic analysis, thereby capturing a wide spread of views and experiences of the deployment of cloud computing .

2. Data Collection

Data collection would follow two stages, namely quantum data and qualitative data collection. The two data collection stages would be carried out using a combination of methods to ensure thorough coverage of the four deployment models of the cloud.

2.1. Quantum Data Collection

Surveys and case studies are used in contacting the various organisations involved in the study to gather data for the quantitative analyses. These are organisations already having at least one of the four cloud deployment models that can be: public, private, hybrid, or community clouds. The step-by-step procedure on the gathering of data is as follows:

1. Questionnaire Design: For closed-ended questions that easily allow quantifying the data, numerical in nature, most of them were cost savings, scalability, data security, and compliance. To obtain responses related to participants' satisfaction toward their preferred cloud model, Likert scales applied here; multiple-choice questions were used to extract detailed demographic and organisational details.
2. Sampling: Organisations for the study are those who have adopted the cloud computing model. The required number of organisations was 200, and the response rate was 65%. Sampling size would ensure satisfactory validity for the collected quantitative data. For achieving heterogeneity, sampling was further bifurcated on a basis of type of industry and size.

3. Case studies: Surveys also had case studies of three organisations that had migrated only recently during the last year from traditional IT infrastructure to cloud environments. Case studies gave real-time data about savings in cost, time, and improvements in performance.
4. Data points accumulated: Some quantitative data includes
Costs incurred for deploying and maintaining the cloud.
Scalability metrics, i.e., servers or storage capacity.
- Response times and uptimes on performance metrics.
- Security incidents like breach or downtime .

2.2. Qualitative Data Collection

Apart from the quantitative data, qualitative data will also be collected as a supplement. This would also help to access more up-to-date and sophisticated scenarios of decision-making and user experience in relation to the deployment models of cloud. The two mainly followed approaches have been semi-structured interviews and focus groups.

1. Semi-structured Interviews: The population consisted of 20 IT professionals and decision-makers, who led the cloud deployment models of their respective organisations. The semi-structured interviews provided flexibility with questions since research participants could elaborate on their experiences, the challenges they had to face, and their opinions on any particular question asked. Questions focused on :
Determinants about which particular cloud deployment model to choose.
Security issues and how these issues were addressed.
Know how the cloud model is beneficial/ detrimental to them.
Problems related to the implementation process, cost, integration with other systems, quality of support from the vendors.
2. Focus Groups: Participants from organisations who employ hybrid or community-based cloud models were sampled for the focus group. There were 6 to 8 participants for each of the focus groups. In general,

focus groups enabled discussions primarily by a facilitator using open-ended, pre-designed questions. Focus groups have also allowed avenues to unravel how disparate approaches towards usage of cloud computing models would impact day-to-day operations, collaboration and access data for end-users.

3. Document Analysis To achieve a more defined insight further in the details, the following internal reports and other documents from the organisations were verified. This research study, thus, helped cross-validate qualitative as well as quantitative data collected from both interviews and focus groups by validating them from documents.

3. Data Analysis

Two steps of data analysis were adopted in this study coinciding with the two stages of data types that had been involved. Different analytical techniques were used in each step to ensure the soundness and validity of results.

3.1. Quantitative Data Analysis

Statistical package for Social Sciences (SPSS) and surveys with case studies were used to analyse the gathered quantitative data. The tool that was mainly employed in analysis was SPSS, which enabled the use of various techniques for the exploration of relationships between different variables, such as cost savings, scalability, security incidents, and cloud deployment model.

1. Descriptive Statistics: The first step should have been to build up the descriptive statistics such as means, medians, and standard deviations to summarise key data points and get an idea about overall trends and distribution regarding cloud deployment models.

2. Comparative Analysis: A one-way ANOVA was also used to compare the effectiveness of various cloud models in relation to each other - public, private, hybrid, and community - with the intention of ascertaining whether the variations were significantly diversified as far as cost efficiency, performance, and security are concerned.

3. Regression Analysis: Multiple regressions were conducted to establish what factors were more significant in affecting the adoption of certain cloud-deployment models. The independent variables used were size of organisation, type of industry, and security issues; the dependent variable was the type of model selected.

4. Correlation: Through correlation analysis, it was possible to look at trends between certain variables. This involved the examination of the correlation between adoption of a cloud model and better performance or lower costs. This way, patterns which could be inferred as causal relationships were established.

3.2 Qualitative Data Analysis

The data in this study had qualitative dimensions and were ascertained through interviews, focus groups, as well as document analysis that was carried out through thematic analysis. The reason for this was because it allows the determination of patterns, reoccurring themes, and relationships within the data.

1. Coding: Data analysis qualitatively begins with coding the interview and focus group transcripts. Coding refers to the reviewing of data where mainly, important statements or phrases are identified and categorised under preliminary codes. Preliminary codes often come out as main themes, such as security concerns, cost-related challenges, and user satisfaction.

2. Thematic Analysis: The codes were then clustered into themes that have captured the soul of the responses given by participants. Thus the different themes "security and compliance", "cost-benefit analysis", "integration issues," "and user experience" obtained in the data set. Based on these themes, the researchers could identify important insights as well as common challenges that have been encountered by organisations in various sectors when adopting cloud deployment models.

3. Triangulation: To enhance the qualitative outcome, triangulation was performed. Using three methodologies-interview, focus group, and document analysis-data gathered were cross-checked and cross-compared to establish consistency or support the findings made. The outcome was that the fact-finding process was strengthened as the qualitative data was made to appear more robust.
4. Tools/Software

Various tools and software have facilitated the collection and analysis of data. These include tools that can handle large datasets, ensure accurate statistical analysis, and particularly support qualitative analysis through coding and theme generation.

4.1 SPSS for Statistical Analysis

SPSS was the core application software deployed in executing the quantitative analysis. SPSS helped the research team perform a number of statistical tests including descriptive statistics, ANOVA, and regression analysis. This tool was used as it could handle large datasets with a possibility of complex statistical calculations and representing the same through graphs or charts.

4.2. NVivo for the Qualitative Analysis

The qualitative data of interviews and focus groups were analysed using the very powerful qualitative data analysis tool, NVivo. It helped the research team effectively organise, code, and text data for analysis. Its features for the identification of themes, word frequency analysis, and data visualisation streamlined thematic analysis and maintained consistency with several data sources.

4.3. SurveyMonkey for Survey Administration

Quantitative data are collected using SurveyMonkey, an online survey tool in which the distribution of the survey is given to a variety of organisations. It has a wide range of personalised options for designing the survey, such as Likert scales, multiple-choice questions, and open-ended responses. Furthermore, it has easy data collection and exportation that one can then import to SPSS for its analysis. We utilised SurveyMonkey to great effect in rationalising the collation process while putting responses into a standardised format.

4.4. Using Microsoft Excel to Process Data

The data was cleaned and organised initially by Microsoft Excel prior to any complex analysis by SPSS. Because Excel was a compact tool that could handle large datasets efficiently, it was a good device to manage and organise the raw data of both surveys and case studies. It also allows some basic statistical functions, especially in running preliminary checks on data-including missing data checks, calculations of descriptive statistics, and even generating pivot tables for preliminary quick comparisons.

5. Ethics and Limitation of Research

This paper articulates the ethics involved in conducting this research and some limitations associated with the study.

5.1. Ethical Considerations

Ethics were crucial when collecting the data and analysing it since the information involves sensitive data about how an organisation implements their clouds. That said, the following was put into consideration to ensure the research was strictly ethical.

1. Informed Consent: All the respondents involved in any survey, interview, or focus group were informed of the purpose of the study, their role, as well as the manner in which their data would be used. All participants gave written consent; they were assured that participation was entirely voluntary and they had every right to withdraw at any time without consequence.
2. Confidentiality and Anonymity: The entire organisations and research study respondents were maintained as confidential. The Information which was identified in nature was anonymized; thus keeping the sensitive details about the organisational cloud adoption strategy or security concerns secret. The data of the participant was safely stored, and only the research team had access to it.

3. Data Protection: Physical data was kept safe in hard format and digital forms encrypted with access allowed only to the permissioned people within the bounds of compulsory law and regulation that provided the protection of data. The research was held in the format of the General Data Protection Regulation (GDPR) format, and collections, processing, and rendition of personal and organisational data came out to be on international standards.

4. Balanced Representation: The study targeted striking a balance of representation of every respondent's idea. Data collection and analysis was not biassed. The interviewers and focus group researchers were trained adequately and managed to take the sessions without raising any suggestive questions likely to manoeuvre responses from the respondents.

5.2. Limitation of the study

Although the mixed-method approach has given a well-rounded perspective about deployment models in cloud computing, there may be some limitations within the resultant findings that make generalisation about the findings for other settings challenging.

1. Sample Size and Generalisability: As many as 130 organisations responded to the survey, but still, the sample size is relatively small in size. Samples could be more vast and varied, and samples could be cross-industry as well as interregional samples in relation to this concept of cloud deployment. The research has mainly been conducted on organisations belonging to the health care, finance, education, and government sectors. Therefore, the results gained here cannot very accurately be applied to the retail industry or manufacturing industry.

2. Self-reported Data: The data for this research is primarily collected using self-reported organisations that rely on their use of cloud resources, and the same may therefore be susceptible to social desirability bias. Organisational representatives may tend to overreport the achievement or security success of their cloud adoptions. In addition, measures were applied using cross checks with internal documents, but discrepancies are likely to exist.

3. Rate of Change of Technologies: Cloud technologies are evolving at a pace that questions the sustainability of findings. Multi-fold growth of cloud computing is taking place; new deployment models like multi-cloud and edge computing emerge and fade out. Inevitably, some of the findings presented would

eventually become obsolete as more and more organisations shift their existing and new systems to new varieties of those technologies and practices in place.

4. Big Companies: The sample for this study was largely dominated by medium to large organisations that in fact may have better resources to use in cloud computing. This focus may actually limit the generalisability of the study towards small businesses or startups and may be able to create a motivated respondent base with different motivations, concerns, and barriers for going to the cloud.

6. Validity and Reliability

Valid and reliable research findings are of tremendous interest in research design and execution. For this purpose, in keeping the study valid, the following strategies were employed:

6.1. Validity

1. Internal Validity: The research took two precautions towards the internal validity of the research: survey instruments were carefully designed to meet the purposes of the study. A pilot test was conducted on a small sample of organisations to detect areas of ambiguity or misunderstanding in the questions. Feedback from this pilot group was incorporated into the improvement of the survey. Only then would the survey be distributed on a full scale.

2. External Validity: Even though the results based on this study are premised on data of specific industries and geographical locations, best attempts have been made to make sure that as varied as possible kinds of organisations with diverse patterns of cloud usage are covered. As such, the study aimed to enhance the external validity of the outcome through inclusion of organisations operating in diverse sectors like the health, education, finance, or government sectors. It would be good if future research studies are extended with some other sorts of industries and geographies for extending these findings in future studies.

3. Construct Validity: The survey instruments and interviews were adequate in capturing the variables of interest; such examples are the questions in the surveys and interview protocol that directly spoke to the topics such as the model for deploying clouds, effectiveness, and the challenges that could be anticipated by organisations when they adopt such models. Sources of data employing that allow the establishment of findings are more construct validity-surveys, interviews, and case studies.

6.2. Reliability

1. Consistency Data Collection: To ensure the validity of the data, formalised techniques in collecting data were applied for both the quantitative as well as qualitative responses. The same questionnaire was used for a survey that was undertaken among the respondents. The questions were posed almost alike in all the semi-structured interviews. Focus groups also were standardised in nature because they were facilitated by an experienced facilitator who led the groups using an a priori set of questions.

2. Inter-coder Reliability: While conducting the analysis of qualitative data, more than one researcher coded interview and focus group transcripts. In order to enhance reliability, inter-coder reliability checks were conducted whereby different researchers coded the same transcripts independently and then compared their decisions to which they applied. Discrepancies that came up were resolved by discussion and consensus in order to achieve uniformity in the thematic analysis.

3. The research methodology, tools of data gathering, coding schemes, and statistical analyses have all been well detailed for replication purposes in subsequent studies. An openness over the method of the research process increases the chances that the results might be replicated under varied contexts or varied samples by other researchers.

IV. RESULTS

We have synthesised findings related to different deployment models of cloud computing: public, private, hybrid, and community clouds. Meta-analysis is synthesised from combined survey, case study, interview, and focus group data for insights into the performance, adoption rate, security implications, cost efficiency, and general satisfaction of each of the above types of cloud deployment.

1. Adoption Trends and Rates

The analysis of the survey data shows clearly defined trends in the adoption of cloud deployment models across sectors. Public clouds were the most used model in organisations, with 45% of respondents adopting public cloud services, because this model is scalable, cost-effective, and very easy to implement. The private cloud was being more and more adopted by finance, education, and health organisations: 30% of the respondents put the private cloud into operation, mainly for security reasons and to fulfil requirements.

Hybrid clouds constitute the rest 25% where they can generate both public and private clouds. Hybrid clouds were largely adopted in business-to-business areas where the demand for data tends to be volatile because of e-commerce and logistics. Community clouds were adopted a little due to the fact that only 10% of the respondents utilised this type of model for governments and research institutions where collaboration from various organisations is required.

2. Performance and Scalability

The survey results show that scalability has been one of the most significant benefits that various cloud deployment models provide. Scalability was reportedly the area in which users of public clouds found satisfaction at the most significant level because 85% of respondents found public clouds to meet or exceed the expected degree of scalability in adapting variable workloads. The primary reasons for choosing the public cloud model were high degrees of scalability and ability to scale on demand in order to meet the sudden spikes in traffic.

However, private cloud users complained that these clouds were not scalable. While 60% of the users of private cloud reported satisfaction about performance, 40% of the users said that they needed much time and spending to scale up the operations where hardware upgrade and technical know-how often provided a bottle-neck. This was mostly for small companies which had limited resources to maintain a scalable private cloud infrastructure.

Hybrid clouds were highly scalable and high-performing but only satisfied 75% of the organisations that undertook the survey. Moving less sensitive workloads to the public cloud while still keeping relevant data in private infrastructure helped in optimum exploitation of resources. Community clouds were low in scalability potential compared to others as only 50% of the respondents expressed satisfaction since community clouds share the infrastructure by default, which is usually limited by collective resources.

3. Cost Effectiveness

There was also great variation in the cost-effectiveness of each cloud deployment model. Cloud services deployed public clouds as the most affordable option for SMEs. 70% of all public cloud users said that public cloud services save them costs compared to their traditional on-premises IT infrastructure. The pay-per-use model kept capital outlays out of the initial costs and presented organisations with an automatically scaled-cost solution.

Private clouds were perceived to be costlier as compared to deployment of private clouds. 65% of the respondents who had adopted private cloud reported that running private clouds is pricier, mainly due to the need for dedicated hardware, software licences, and IT staff. In many cases, organisations with strict data security and compliance needs, such as healthcare and finance had to do the cost justification by themselves.

Hybrid clouds were a compromise between expenditure and performance as 60% of respondents felt that the cost savings from utilisation of public cloud resources were greater than the higher setup costs of establishing a private cloud. Community clouds had even higher operational expenses compared to their cost effectiveness with 55% of organisations finding expenses that were higher than initially anticipated mainly because of the added complexity in managing a shared infrastructure shared across multiple stakeholders.

4. Security and Compliance

Security and Compliance

Security is still an extremely important consideration for cloud-based services, particularly for highly regulated industries. Security is where private cloud deployments scored the highest. From the healthcare and finance industries and from the respondents from government offices, 90 percent said they had the confidence to meet tough compliance requirements. Among the reasons cited as reasons for adopting private clouds were the ability to provide customised security layers as well as full control over data.

Public clouds are supposed to offer a pretty safe security environment, though they are deemed to be significantly riskier, primarily by the organisations that handle highly valued, private, or regulated information. One of those issues in users' data privacy and regulatory compliance is what 40% of them, especially those industries subject to GDPR, shudder at the thought of. Hybrid clouds acted as a temporary solution, as 80% of the respondents reported satisfaction with the security posture by segregating sensitive workloads in private clouds while public clouds are used for less sensitive tasks.

Respondents pointed to specific security concerns: community clouds, 45% of respondents noted that it is because of the shared nature of infrastructure and lack of control over access. Community clouds often feature security robust frameworks to address the relevant regulatory compliance requirements; handling cross-functional access control across a plurality of business organisations was one of the most common issues that participants brought up.

5. Customer Satisfaction

Customers' expectations are measured on performance, security, scalability, and cost dimensions. In all these aspects, public clouds ranked the highest for average overall satisfaction rate: 80 percent reported having met or exceeded their expectations. Private clouds scored very high in regard to security and compliance but scored low on scalability and cost-effectiveness; 70 percent of users are satisfied. Hybrid clouds are valued due to their flexibility and low cost, with 75 percent of users satisfied. Community clouds scored mixed with 55 percent of respondents satisfied based on concerns on control and security shared.

Aspect	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud
Infrastructure Ownership	Owned by third-party service providers	Owned and managed by a single organisation	Combination of public and private clouds	Shared by multiple organisations with common needs
Cost	Low initial cost, pay-as-you-go pricing	High setup and maintenance costs	Moderate cost (mix of both public and private)	Shared cost among participating organisations
Security	Lower security control, data shared across multiple tenants	High control, dedicated infrastructure	Security depends on which parts use public vs. private cloud	Moderate, shared responsibility among participants
Scalability	Highly scalable, almost unlimited resources	Limited by in-house resources	Scalable in public portion, limited in private part	Scalable within community but more restricted than public cloud
Customization	Limited customization options	High level of customization	Some customization, depending on the mix	Moderate customization, based on shared needs
Compliance	May not meet strict regulatory requirements	Designed to meet strict regulations	Sensitive data kept in private cloud, non-sensitive in public	Meets specific industry or regulatory compliance
Management Complexity	Minimal management required	High management effort	Complex management due to integration of public and private	Moderate complexity, with shared governance among organisations
Usage Scenario	Suitable for SMEs, startups, and general businesses	Ideal for large enterprises and government	Ideal for businesses with fluctuating workloads	Suitable for industries with similar regulatory needs (e.g., healthcare)
Data Control	Limited control over data	Full control over data	Partial control (full in private cloud)	Shared control, collaborative governance
Latency	Higher latency due to shared infrastructure	Low latency, localised infrastructure	Variable latency (depends on public/private usage)	Moderate latency, depending on shared network conditions

V. CONCLUSION

These models describe cloud computing deployments into public, private, hybrid, and even community clouds. Various benefits and challenges that these types of models have are discussed based on their performance, scalability, cost-effectiveness, security, and even user satisfaction levels.

Public clouds are the most scalable and cost-effective option suitable for smaller organisations as well as those with fluctuating workloads. But, in regulated sectors, there are major restrictions to their greater usage due to security issues. True, private clouds offer superior control and compliance capabilities but at a higher cost and less scalable. Hybrid clouds leverage the best of both worlds and combine them for flexible options for organisations interested in balancing security with cost and performance. However, community clouds are promising, but they have a tough road to handle due to governance and shared security responsibilities.

Therefore, depending upon the specific needs and requirements of an organisation along with industry needs and resource availability, an appropriate cloud deployment model can be selected. The future research directions should include emerging models like multi-cloud strategies and edge computing to get an overall perspective on the landscape of a cloud.

REFERENCES

[1] Mell, P., 2011. The NIST Definition of Cloud Computing. *NIST Special Publication*, pp.800-145.

[2] Hamid, H.A. and Yusof, M.M., 2015. State-of-the-art of cloud computing adoption in Malaysia: A review. *Jurnal Teknologi*, *77*(18).

[3] Abdullah, J.L. and Seng, L.C., 2015. Acceptance of cloud computing in Klang Valley's health care industry, Malaysia. *International Journal of Economics, Commerce and Management*, *3*(6), pp.392-415.

[4] Alharbi, F., Atkins, A. and Stanier, C., 2016. Understanding the determinants of Cloud Computing adoption in Saudi healthcare organisations. *Complex & Intelligent Systems*, *2*, pp.155-171.

[5] Ahmadzada, S., Zayyad, M.A. and Toycan, M., 2016, October. Readiness assessment for the use of cloud computing in eHealth systems: a field study of hospitals in the capital of Azerbaijan. In *2016 HONET-ICT* (pp. 141-144). IEEE.

[6] Gupta, P. and Kulkarni, N., 2013. An introduction of soft computing approach over hard computing. International Journal of Latest Trends in Engineering and Technology (IJLTET), 3(1), pp.254-258.

[7] Mokhtar, S.A., Ali, S.H.S., Al-Sharafi, A. and Aborujilah, A., 2014, December. Organizational Factors in the Adoption of Cloud Computing in E-learning. In *2014 3rd International Conference on Advanced Computer Science Applications and Technologies* (pp. 188-191). IEEE.

[8] Lian, J.W., Yen, D.C. and Wang, Y.T., 2014. An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), pp.28-36.

[9] Kusnandar, T. and Surendro, K., 2013, June. Adoption model of hospital information system based on cloud computing: Case study on hospitals in Bandung city. In *International Conference on ICT for Smart Society* (pp. 1-6). IEEE.

[10] Noor, T.H., 2016. Usage and technology acceptance of cloud computing in Saudi Arabian Universities. *International Journal of Software Engineering and Its Applications*, *10*(9), pp.65-76.

[11] Pocatilu, P., Alecu, F. and Vetrici, M., 2010. Measuring the efficiency of cloud computing for e-learning systems. *Wseas transactions on computers*, *9*(1), pp.42-51.

[12] Bani-Salameh, H. and Fakher, S.A., 2015, November. E-learning critical success factors model: Empirical investigation. In *Proceedings of the International Conference on Intelligent Information Processing, Security and Advanced Communication* (pp. 1-6).

[13] Shahzad, A., Golamdin, A.G. and Ismail, N.A., 2016. Opportunity and challenges using the cloud computing in the case of Malaysian higher education institutions. *The International Journal of Management Science and Information Technology (IJMSIT)*, (20), pp.1-18.

[14] Badie, N. and Dahlan, H.M., 2014. Cloud computing adoption factors for university administration. *Jurnal Teknologi*, *70*(5).

[15] Al-Arabiat, D., Ahmad, W.F.W. and Sarlan, A., 2016, August. Cloud computing role to address mobile learning barriers: An exploratory study of HEIs in Malaysia. In *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)* (pp. 553-558). IEEE.

[16] Alassafi, M.O., Alharthi, A., Walters, R.J. and Wills, G.B., 2016, October. Security risk factors that influence cloud computing adoption in Saudi Arabia government agencies. In *2016 International Conference on Information Society (i-Society)* (pp. 28-31). IEEE.

[17] Wahsh, M.A. and Dhillon, J.S., 2015, December. An investigation of factors affecting the adoption of cloud computing for E-government implementation. In *2015 IEEE Student Conference on Research and Development (SCOReD)* (pp. 323-328). IEEE.

[18] Elena, G. and Johnson, C.W., 2015. Factors influencing risk acceptance of cloud computing services in the UK government. *arXiv preprint arXiv:1509.06533*.

[19] Abdollahzadegan, A., Che Hussin, A.R., Moshfegh Gohary, M. and Amini, M., 2013. The organizational critical success factors for adopting cloud computing in SMEs. *Journal of Information Systems Research and Innovation (JISRI)*, *4*(1), pp.67-74.

[20] Mohammed, F. and Ibrahim, O., 2013. Refining e-government readiness index by cloud computing. *Jurnal Teknologi*, *65*(1).

[21] Hellstén, S.M. and Markova, M., 2006. The DeLone and McLean model of information systems success-original and updated models. In *SIGCHI Conference* (pp. 1-5).

[22] Petter, S., DeLone, W. and McLean, E., 2008. Measuring information systems success: models, dimensions, measures, and interrelationships. *European journal of information systems*, *17*(3), pp.236-263.

[23] Rana, N.P., Dwivedi, Y.K., Williams, M.D. and Weerakkody, V., 2015. Investigating success of an e-government initiative: Validation of an integrated IS success model. *Information systems frontiers*, *17*, pp.127-142.

[24] Gangwar, H., Date, H. and Ramaswamy, R., 2015. Developing a cloud-computing adoption framework. *Global Business Review*, *16*(4), pp.632-651.

[25] Mohammed, F. and Ibrahim, O., 2015. Models of adopting cloud computing in the e-government context: a review. *Jurnal Teknologi*, *73*(2).

[26] Ahmad, T. and Waheed, M., 2015. Cloud Computing Adoption Issues and Applications in Developing Countries: A Qualitative Approach. *Int. Arab. J. e Technol.*, *4*(2), pp.84-93.