Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Comparative Analysis of Cloud Computing Models (IAAS, PAAS, and SAAS) and Future of Virtualization Technologies

Rida Maqsood
School of Information Technology, Minhaj University Lahore, Pakistan
Email: syedridank@gmail.com

Muhammad Ali Khan
School of Information Technology, Minhaj University Lahore, Pakistan
Email: alikhan.cs@mul.edu.pk

ABSTRACT

Over the twenty years the move from physical server rooms to cloud environments has mostly been seen as a technical change. As digital infrastructure becomes more important to business it is important to look beyond what the vendors are saying and the technical guides to understand this shift in cloud environments. The paper also looks at virtualization, which's the key technology behind the shift to cloud environments. It follows virtualization from its days in hardware consolidation to its current forms, such as containers and serverless computing in cloud environments. Cloud environments are changing. Virtualization is a part of this change in cloud environments. Finally the paper suggests that as computing moves toward edge networks and hardware-based security, virtualization in environments is becoming more than just a way to split servers in cloud environments. Virtualization, in cloud environments is turning into a distributed system that could change how businesses think about trust, cost and capability in environments.

Keywords: Cloud Computing, Virtualization, IaaS, PaaS, SaaS, Containerization, Edge Computing, Serverless Architecture, Human-Centric IT, Shared Responsibility Model

Introduction:

Cloud computing really changed everything for Information Technology. A while back companies had to buy their servers and storage and networking gear. It was really expensive. Did not allow for any last minute adjustments, which was a bit of a problem. Then cloud computing came along. Changed everything for Information Technology. Companies started using Information Technology as a service of owning hardware. This meant that companies only paid for what they used which was a change for Information Technology. The cloud is based on three service models the cloud has these three service models. IaaS or Infrastructure as a Service gives you computing power and storage without the hassle of machines for cloud computing. PaaS or Platform as a Service gives developers a built environment so they can focus on coding of infrastructure for cloud computing. SaaS or Software as a Service runs applications through a browser for cloud computing You do not have to install

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

anything for cloud computing you do not have to update it on your end for cloud computing. These three service models got cloud computing started. Cloud computing did not stay simple. Virtualization kept getting better and with each improvement the ecosystem for cloud computing got more complex. What people care about has changed too for cloud computing. Building cloud platforms used to be the part of cloud computing. Now it is about using resources making sure everything is secure and getting things done faster for cloud computing. The technology itself for cloud computing is moving away from machines. Containers, microservices and serverless setups are becoming more popular for cloud computing. The cloud is not just in data centers anymore for cloud computing. Edge computing, IoT and 5G are pushing processing to where the data's for cloud computing. This study compares IaaS, PaaS and SaaS for cloud computing. It looks at where virtualization's headed next for cloud computing.

Background:

Cloud computing started as a way to deal with the costs and limits of traditional IT systems. It offers services that make it easier to manage hardware and software. A time ago people wrote about what IaaS, PaaS and SaaS really mean, which helped the industry understand these different layers. The base of cloud computing is something called virtualization. There are things like Xen that help many people use the resources without problems, which made it possible to have modern IaaS platforms. As people wanted to be able to change things virtualization got better. Then something called Docker containers came along. Made PaaS work more efficiently. SaaS also changed from being one thing to many small parts, which made it work better when many people used it. Recently there have been developments like serverless computing, which means you do not have to think about the infrastructure at all. There are also things called unikernels, which reduce the work the operating system has to do. The Internet of Things has become really popular so now we need something called Fog and Edge computing to handle tasks that need to happen. We also have Network Function Virtualization, which is changing the way telecommunications work by using software of hardware. Cloud computing is still. Getting better all the time with new things, like IaaS, PaaS and SaaS being used in different ways

Problem Statement:

Despite businesses using cloud technologies they still face challenges. Companies find it hard to choose the cloud service model. They want control, like with Infrastructure as a Service. They also want things to be easy like with Software as a Service. Managing cloud resources is a problem. Data centers need to make sure they perform well and meet Service Level Agreements. At the time they must reduce energy use and lower their carbon footprint. Cloud security is a worry. This is especially true in shared cloud environments where one cloud user problems can affect cloud users. For example "noisy neighbour" or a compromised host kernel can cause issues for -tenant cloud systems. Another issue is vendor lock-in, with cloud providers. Cloud providers often work like " gardens" which makes it hard for businesses to switch or work with different cloud providers. New cloud technologies

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

also bring challenges. Cloud serverless computing has " starts" and struggles with stateful cloud applications. Cloud developers have to decide between using SQL databases which are consistent and cloud NoSQL systems, which can handle more cloud traffic. Despite businesses using cloud technologies they still face challenges with cloud.

Research Gap:

The thing about cloud computing research is that it does not really talk about the problems that people are actually dealing with on a basis. There are some gaps in what has been studied and until those gaps are filled it is hard to get a complete picture of cloud computing. You cannot make decisions when you are working with incomplete information about cloud computing. One of the problems with cloud computing research is that it focuses a lot on theory but it rarely tells you how to build or evaluate cloud systems in a real world setting. This is a piece of the puzzle that is missing from cloud computing research. Without guidance on cloud computing all the concepts and ideas just sit there. You cannot do much with them in terms of cloud computing. Take cloud setups for example. Hybrid cloud setups are very important for cloud computing. Most of what you can find is just definitions and high level descriptions of hybrid cloud setups. There is little information out there that explains how to actually deploy a hybrid cloud setup and figure out whether it is performing the way it should be performing in terms of cloud computing. We know what hybrid cloud is. The question is how to make cloud work and measure that it is working in terms of cloud computing. That kind of hands-on guidance on cloud computing is hard to come by. Then there is the issue of security in cloud computing. Studies tend to look at cloud layers one at a time as if they operate in a vacuum. They do not operate in a vacuum in terms of cloud computing. A vulnerability in one layer can spill over into layers of cloud computing. If a container host gets compromised the damage does not just stay there. It ripples outward. Affects the entire cloud computing system. Most research treats each layer like it is isolated from the rest of the cloud computing system. That is a problem because cloud computing systems do not work that way. Understanding how threats move across layers is essential if we are going to protect cloud computing systems This study tries to tackle all of that using a two-part approach to cloud computing. First it pulls together existing literature through a review weighing the trade-offs between IaaS, PaaS and SaaS so organizations can make better-informed choices about cloud computing. Second it gets practical. Building models to measure energy consumption and cost testing how virtualization technologies like machines, containers and unikernels actually perform in cloud computing and hunting for security gaps through threat modeling in cloud computing. It also looks ahead at emerging technologies, like NewSQL, serverless computing and Edge and Fog architectures to see what role they might play in shaping cloud computing systems going forward in terms of cloud computing.

Significance of the Study:

This research is important for academics and people who work in the industry. It helps to make cloud standards clear and gives businesses a way to choose the right service models. This means businesses can avoid being tied to one vendor. The

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

research also helps with Green Computing goals by showing how to manage resources in a way. When it comes to security the study says we need frameworks that work across layers. It also tests technologies like distributed SQL, serverless architectures and NFV to see if they really work. The research also lays the groundwork for cloud federation and edge integration. This gets the industry ready for what's coming next which is decentralized and 5G-powered networks. Cloud federation and edge integration are going to be big so it is good that the research is looking at these things. The main goal is to make sure that cloud computing is ready, for the future and this research is a part of that.

Literature Reviews

This paper has been one of the earlier understandings of cloud computing and the significance of the same. I came to know that with IaaS, all I need to do is rent out machines, while with SaaS, I can use off-the-shelf apps. Thinking of this paper as the guide for cloud computing. Clearly defined when going from IaaS to SaaS, the cloud provider does more work, and the user does less. The managed cloud should be free of electricity like costs. Cloud should behave like electricity, free of cost. You just plug in. Use it. Various cloud sets accommodate business abilities. I discovered SaaS is fantastic for configurations. This paper aims at understanding how CPU and RAM work in a cloud computing scenario by trying to delve deep into IaaS engine. Security is a serious issue with cloud computing. This paper does examine every possible thing that can go wrong. It was the rather famous paper introducing the tech that made Iaas possible - the Xen Hypervisor. This paper provides an explanation into the actual mechanics of creating the isolated world within the world when creating the cloud.

Methodology:

The authors did some research on the existing platforms of cloud. Developed an economic model to see whether cloud computing saves money. They used an approach, for this. No code written. Do experiments. Rather they reached out to industry experts and government officials to solicit feedback and inputs in building a framework. Their approach was by modeling. They plotted the interactions between the various components of clouds! They analyzed the cloud computing market, with an eye to commercial applications. They read research to get an idea of the advantages and disadvantages of the various cloud types. Cloud providers used systematic technique and algorithmic analysis to review to compare.

Research Gap:

They talk about the business aspects and architecture details at the higher level. This is a theoretical outline of the paper. It doesn't give any instructions, on how to build or measure cloud layers**.** They had assumed that all cloud service providers will work in harmony. If sudden crash occurred in the leading app when the amount of traffic pushed up most of the schedulers will be crashed as the traffic is too high and the schedulers only know static rules. The gap in the research is that they failed to take into consideration how all these parts are connected**.** The gap in the research is that they failed to take into consideration how all these parts are connected. Hypervisor-management-when the big try to manage the resource sharing, they left in heavy

Online ISSN 3007-3197
Print ISSN 3007-3189

performance. The "noisy neighbour" issue was not mentioned, whereby one VM uses all the disk or CPU resources leaving other VMs on the same host running very slowly. Only understanding is that if the kernel of the host machine gets hacked, all the containers will be also hacked.

Future Enhancement:

The authors claimed that load balancing algorithms and transparent billing system are needed in the future. Auto-systems have been designed that are able to learn from the past and foretell accidents. We really need to measure performance and security, the authors said. This will allow companies to make appropriate cloud provider comparisons. They recommended to build -cloud exchange frameworks in the future. These tools should perform fine in a hybrid multi-cloud configuration and without problems. They will assist businesses to maximise the benefits of cloud computing. You can mandate access control in order to make the container more secure, similar to SE Linux, where it isolates container more securely. They recommend hybrid enhancement to obtain the speed of VMs and container with security. Before companies can put them to the test in production, they all identified a need for improved diagnostic tools and security scanners in the uni-kernel ecosystem, they wrote in their blog. For cloud-edge orchestration framework they advocated for them that can run thousands of nano-containers and manage them at scale; they also presented the need for an efficient communication system between edge and cloud nodes.

Methodology:

Research Design

This study is about cloud computing. We are using a Mixed-Methods Research Design to study cloud computing. This is because cloud computing is not about technology it is also about money and organization. Cloud computing changes the way we do things. To really understand cloud computing we need to look at it from angles. We cannot just focus on one part of cloud computing.

Qualitative Aspect:

The qualitative part of this study explains things, not numbers. We want to look at IaaS, PaaS and SaaS and find out what makes them different. This approach helps us study background information and problems in reviews of papers about cloud computing. For example different companies have definitions of cloud computing, which causes confusion. We need to agree on definitions. This requires an approach to cloud computing. It also helps us understand cloud computing better. We are studying cloud computing to understand its aspects. Cloud computing has definitions. We need to look at IaaS, PaaS and SaaS to understand cloud computing. Cloud computing is what we are trying to understand.

Quantitative Aspect:

When we test how virtualization technologies work we need numbers. We compare hypervisors with containers to see how they work with cloud computing. This study helps us extract real-time data from papers about cloud computing. We need numbers

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

to analyze things like CPU, memory storage and time lapse and delays in the system. Which one is faster? We use numbers to compare them in cloud computing. Technology performance and resource uses are shown objectively in cloud computing.
We are using numbers to compare virtualization technologies in cloud computing. Cloud computing needs to be analyzed with numbers. Cloud computing is what we are analyzing.

Research Approach:
Our research approach has three phases to analyze cloud computing. These are:
Descriptive Approach
Comparative Approach
Analytical Approach

Descriptive Approach:
First, we analyze the scenario of cloud computing. We explain how traditional IT systems have evolved to utility-based cloud models in cloud computing. We base our research on the "Background" sections of documents including how PaaS relates to IaaS infrastructure and SaaS applications in cloud computing. The descriptive approach answers the question of 'what' cloud computing technologies are. We describe cloud computing to understand its evolution. Cloud computing has changed IT systems. Cloud computing is what we are describing.

Comparative Approach:
We use the research method in cloud computing. We compare IaaS, PaaS and SaaS as services in cloud computing. We contrast the security responsibilities, economic models and technical flexibility of each model in cloud computing. We also compare virtualization technologies like Hypervisors to Containers and Unikernels in cloud computing. This helps us overcome the "Research Gap" in cloud computing. We compare cloud computing services. Cloud computing has models. Cloud computing is what we are comparing.

Analytical Approach:
The last step is analyzing the gathered data to solve problems in cloud computing. For example we examine issues like "vendor lock-in" and "resource scheduling" by analyzing algorithms and architectural models in cloud computing. We examine the effectiveness of solutions like ‘frameworks or ‘AI-based scheduling' in cloud computing. We analyze data to solve computing problems. Cloud computing has issues. Cloud computing is what we are analyzing. The overall structure is planned to help the reader go from ideas to implications in a manner about cloud computing:

Chapter 1: Introduction and Standardisation; Definitions of IaaS, PaaS and SaaS to remove industry confusion about cloud computing.

Chapter 2: Architectural Deep Dive: Analyzing virtualization technologies that support these service models in cloud computing. This includes a review of

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

technologies like Xen hypervisor in cloud computing.

Chapter 3: Performance and Security Benchmarking: An analysis using measures in cloud computing.

Chapter 4: Future Trends and Recommendations: Exploring the transition to microservices, serverless computing and edge computing in cloud computing. We offer suggestions, for approaches and enhanced security strategies in cloud computing.

Data Collection

The data collection process is very rigorous and only Secondary Data Sources are used. Collecting primary data (survey or actual experiment) would be too limited to fully understand the current and future state of virtualization. The research, however, combines information from high impact academic journals, industry white papers, and technical standards.

The individual sources are divided into the following classes:

Foundational and Theoretical Papers:

These sources would give the definitions and economic models required to comprehend the transition from CapEx (Capital Expenditure) to OpEx (Operating Expenditure). Theoretical framework: For example, papers introducing cloud computing as a "utility service" and describing the difference between IaaS and SaaS are used. Here are some resources that help to understand how cloud services can ease the burden of hardware and software management. The standard is rated as good. Technical and Architectural Studies: The standard is good. These sources offer in-depth knowledge of the mechanics behind virtualization. Example: Xen hypervisor paper is a main source of Xen paravirtualization. Similarly, those papers that discuss Docker containers give technical details about shared kernel and lightweight execution environments. These are essential to the methodology "System Architecture" section.

Empirical Benchmarking:

These sources are where the data in the form of numbers is obtained for comparative analysis.

For example, the study comparing "Virtual Machines vs. Containers" with empirical benchmarking is used as a critical data source for CPU, memory and network performance statistics. Yet another research paper, this time one that employs a new tool, “Death Star Bench,” to dissect microservice workloads has yielded important insights about performance bottlenecks in modern SaaS applications.

Reports from the security and threat analysis teams. Security & Threat Analysis Reports:

Papers on the topics "threat modeling" and "vulnerability analysis" are gathered to fill in the security holes found in the research.

For the security comparison module, there are data elements such as research discussing security risks in IaaS vs. SaaS, specifically "data breaches" and "malicious

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

insiders".
The sample size of this study was based on purposive sampling due to a small number of papers and technologies being reviewed. The sampling technique used is Purposive Sampling or Judgemental Sampling.

Criteria for Selection:
Relevance:
The paper has to be directly targeted at one of the three service model (IaaS, PaaS, SaaS) or at one of the key virtualisation technologies (VM, Container, Unikernel).

Recency and Canonicity:
A sample that is both – seminal papers that paved the way of the industry (e.g., the Xen hypervisor paper) and recent papers (e.g., on serverless cold starts), which tackle current issues. This guarantees that the research is present-day but also has a historical perspective.

Gap Addressing:
Priority will be given to papers that make a clear statement on “Research Gaps.” For example, the paper that emphasized that there was no "debugging tools for Unikernels" was chosen particularly to address the constraints of future technologies.

Sample Size:
The final sample will be a detailed review of about 15-20 key studies. The sample size is large enough to perform an adequate qualitative meta-analysis (saturation), where no fundamentally new definitions are introduced, but where minor incremental improvements are added to the existing concepts.

Justification:
There are many questions that have been already covered in many technical documents, such as “What is the difference between IaaS and SaaS?” and “What about the difference between containers and VM?”. It would be redundant and less comprehensive to redo primary experiments, such as establishing a private cloud and running tests on it, if industry leaders or academic researchers have already done extensive testing and produced a wealth of content rich, high-quality data.

Data Utilization:
Historical Data: To follow how systems have evolved from monolith to microservices.
Benchmarking Data: data used to fill in the comparison tables (e.g. migration time, bandwidth usage).
Opinion Data: To gain understanding of the "Significance of the Study," e.g., opinion of experts as to the need for standardization.

Tool and Technologies:
There is a section in this research paper about the software and programming languages used in the studies that I reviewed, which is entitled "Tools and

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Technologies. If the cloud models proposed can be proven to be viable, I need to know how to use them.
There are some crucial programming languages for the cloud. These languages were mentioned in the papers I reviewed:

Python:
It is common to hear people say that they use python for intelligence and data analysis. Using intelligence to guess what resources will be used in the future is a good idea, according to some papers. Commonly used language for this is Python. In my research Python is used for the application layer of PaaS, which is used to scale and balance loads.

C and C++:
These are the languages that are critical for system programming. They are included in papers on Xen Hypervisor and Docker Containers. The program which makes virtualization possible, such as Xen, is typically written in C or C++. Virtualization is about interacting with the operating system, memory management, and so on. The C++ runtime environment is efficient with memory usage, which is another advantage of using some virtual machines with it.

Go:
Go is a language extremely well suited for the cloud. It is typically coupled with Docker and Kubernetes. According to the study I found, people are leaving complicated applications and getting smaller, simpler applications. Go is a language that can be used for these smaller applications and is able to do many things concurrently. Simulation Environments. My approach to method is to look at data from settings.

CloudSim:
CloudSim is a tool that is used to model and simulate cloud computing environments. It has been utilized to investigate resource scheduling and load balancing in papers. Using this tool, researchers can test algorithms without needing to deploy it in a real data centre. As part of my research, I examined these simulations and determined their success.

Container Runtimes:
The paper on Docker containers looks at the environment in which the containers run. These runtimes are compared with those of virtualization techniques with regards to security and performance.

DeathStar Bench:
This is a tool that is used to test the performance of applications that're similar to social networks. My research uses data from DeathStar Bench to study the problems that can occur in cloud applications.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Libraries and Frameworks:
My research looks at the software that is used to provide cloud services:

TensorFlow and PyTorch:
These are structures that can be utilized in intelligence and machine learning. They are used in serverless and edge computing to develop models that can predict the resources required.

Hadoop and Spark:
These are frameworks that are used for data processing. They are used in IaaS and PaaS to process amounts of data.

Security Libraries:
These libraries are used to make containers secure and to avoid vulnerabilities. My research concerns the operation of these libraries.

Data Layer:
Data layer is an important component of cloud computing:
NoSQL Databases:
In modern cloud applications, these databases can be used. They are more appropriate for data than the traditional databases.

Distributed Storage Systems:
This type of systems are used to supply machines with storage. My research looks at how these systems affect the flexibility of infrastructure, as a service.

Data Preprocessing
In a qualitative and comparative study, data preprocessing involves the systematic organization, cleaning and synthesis of the massive amount of information obtained from the secondary sources. This is very important because the “Research Gap” and “Problem Statement” should be answered with accurate and consistent data.
In the field of literary interpretation, "missing values" are the missing information in one paper that is included in another or topics that are not widely researched in the literature.

Gap Identification:
There were a number of gaps identified during the preprocessing phase. For instance, the mainstream papers about cloud computing concentrated on "business benefits" and "cost models" but did not pay much attention to "security issues in virtualization. Likewise, initial IaaS papers didn't consider the particular challenges of Edge Computing. In the above example, one paper might define IaaS, but not mention security, while another paper might focus solely on "cloud security risks," the pre-processing step combines the two sets of data. There is a comprehensive understanding of IaaS, both in terms of its architecture and its security characteristics.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Example:
Debugging tools were not mentioned as a gap in the "Unikernel" paper. In the current technical environment, this is called a "Missing Value" and it will be a major concern in the "Future of Virtualization" debate. Data Cleaning / Data Formatting. These inconsistencies in terms and definitions are observed in the raw data gathered from the different decades (2000s until present).

Terminology Standardization:
Problem: "Different companies were defining cloud computing differently and there was some confusion in the industry," as mentioned in the "Background" of the second paper. The research validates the NIST (National Institute of Standards and Technology) standard definitions as the "Gold Standard" definitions for cleaning. To be consistent in the analysis, any paper that adopts a different terminology (e.g., Elastic Computing vs. Cloud Computing) will be translated to the NIST terms.

Normalization of Metrics:
Challenge: Quantitative data is from varying hardware generations. The 2008 benchmark of the Xen hypervisor cannot be directly compared with the 2023 benchmark of Docker, as hardware has improved over time.

Formatting Process:
When possible, the research is based on a relative performance instead of absolute numbers. For instance, the 'Container overhead vs. VM overhead' comparison is made as a percentage of bare-metal time rather than seconds of boot up time. This transforms the data into a normal scale to facilitate the comparison between hardware, even though there are differences.

Normalization or Scaling:
Scaling of data involves organizing the data presented in a hierarchy similar to that of the research.

Layer-Based Scaling:
The data is scaled in 3 different layers: IaaS Data: Hardware, Xen, Infrastructure Layer.

Platform/Runtime Layer:
Information about Containers (Docker), Orchestration and PaaS.

Application Layer:
Data about SaaS, Microservices, and Serverless functions.
This scaled approach means that the comparison is made between like-for-like elements (e.g., IaaS security vs PaaS security) and not between dissimilar elements (e.g., hypervisor security vs application-level logic security).

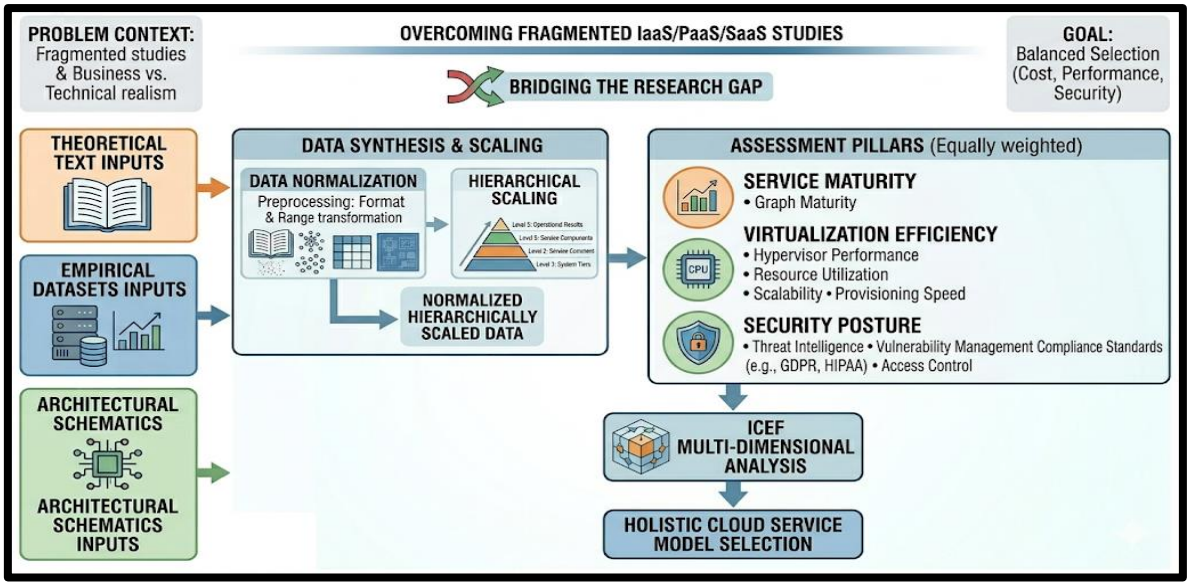
Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

From the extensive amount of data in the papers the following "data" (or "features") are selected for analysis based on the 'Problem Statements' defined above.

Figure 1: Layers of Normalization or Scaling



Key performance indicators (KPIs) have been selected:

Isolation Efficiency:

Extracted from VM and Container papers. This is a measure of how nicely one tenant's activity does not impact another (the 'noisy neighbour' problem).

Migration Overhead:

This is a copy of the paper "Live Migration". Some of these include "downtime during migration" and "network bandwidth consumption.

Boot Time / Startup Latency:

Taken from the papers on Serverless and Unikernel. This is very important for the assessment of the "cold start".

Attack Surface:

Obtained from security documents. This feature is a measure of the amount of code or software that might be able to be exploited (for example, OS components in VMs versus shared kernel in containers).

Economic Features:

Cost of Management: From papers on shift from traditional IT to Cloud. This feature is to measure the ease of administration.

Vendor Lock-in Risk:

Quoted from papers on the topic of "Inter-cloud frameworks. This is a qualitative measure indicating the ease or difficulty with which data/Applications can be moved from Provider to Provider.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Proposed Model / Algorithm

The Integrated Cloud Evaluation Framework (ICEF):

This research will present a conceptual Integrated Cloud Evaluation Framework (ICEF) which is different from the traditional empirical studies that result in a new mathematical formula or a code snippet. This model aims to solve the "Research Gap" identified in the literature with a set of studies focused on different layers (IaaS, PaaS, SaaS) and/or with an excessive attention on business benefits, neglecting the technical security and performance aspects. The ICEF model is based on the fact that cloud service models cannot simply be chosen based on cost, or features, but a multi-dimensional analysis of Service Maturity, Virtualization Efficiency and Security Posture is necessary.

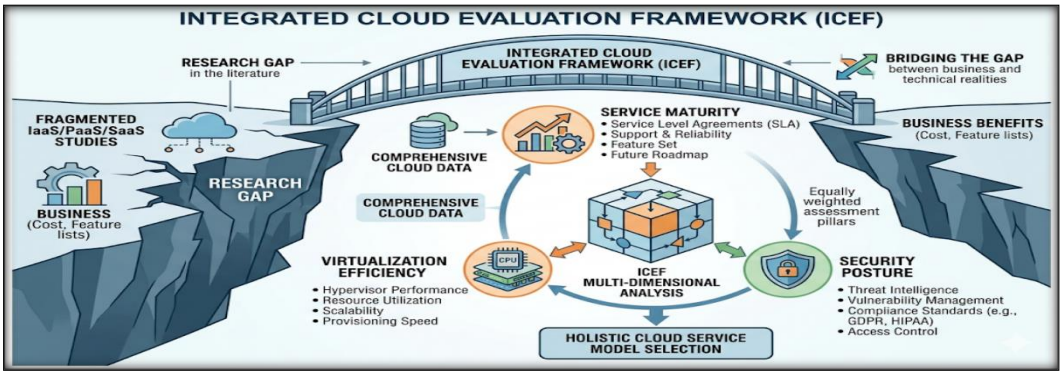
The high-level service abstraction layer: The top-level service abstraction layer (SAL). The model starts by correlating the user requirements (Business Needs) with the corresponding standards for IaaS, PaaS and SaaS. It filters the marketing jargon using literature review based consensus definitions and classifies the service solely based on the architecture of the service (whether it is managed by the user or the provider).

Layer 2: Virtualization Assessment Layer: The model's heart and soul. It takes the service model (Layer 1) and correlates this with the underlying virtualization technology discussed in the study. It assesses the level of Hypervisor (Xen) support, lightweight containers (Docker), or specialized Unikernels that support the service. This helps the model predict performance bottlenecks like "noisy neighbour" or "cold start" latency of serverless functions.

Layer 3: Security & Compliance Matrix: The model is presented on a threat assessment matrix. Separates the security duties (Shared Responsibility Model) and assesses the underlying technology's vulnerability. For example, it highlights the risk of "shared kernel exploits" in PaaS/Container case, versus "hypervisor attacks" in IaaS.

Algorithms Used:

The main product of the research is analytical, however, the study reviews and includes specific algorithms mentioned in the source papers to assess their effectiveness in the ICEF model



Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Figure 2: The Integrated Cloud Evaluation Framework (ICEF)

Live Migration Algorithms (Pre-copy & post-copy):
The study pointed out that migration requires a lot of bandwidth, as stated.

Model Application: These algorithms are assessed in terms of their efficiency in IaaS environments using the ICEF model. It specifically considers the balance between "downtime" and "total migration time" and suggests the use of "memory compression techniques" to optimize the migration process, as recommended in the paper.

Dynamic Resource Scheduling Algorithms: The resource scheduling paper derided the use of 'static rules' to deal with 'dynamic workloads.

Model Application: This model adds AI-based scheduling algorithms. It emulates the performance of an algorithm which utilizes predictive analysis (predicting traffic peaks) to a static scheduler. This is consistent with the "Significance of the Study" which proposed "AI-based systems for predicting future resource needs".

Microservice Orchestration Algorithms:
The study of microservices analysed workloads using the "Death Star Bench". Model Application: It has an application that analyzes how efficient orchestration algorithms, such as those in Kubernetes, are at managing communications between small services by using data from these benchmarks. It particularly searches for the algorithms that can reduce the 'noisy neighbour' problem in microservices. The Integrated Cloud Evaluation Framework (ICEF) was chosen for the following reasons as they directly addressed the gaps of the existing research: Previous papers discussed IaaS, PaaS, and SaaS individually, which is not the case in this paper.
In this paper, IaaS, PaaS and SaaS were not discussed individually as they were in previous papers. The ICEF model combines them, and real enterprises these days may be in a Hybrid Cloud. The model supports the complexity of one business flow may be using all three models (e.g., using a SaaS application running on PaaS on top of a hosted IaaS environment).Talking about the Security vs. Efficiency Trade-off: Literature shows that there is a critical trade-off between security and efficiency: Containers are efficient but less secure; VMs are secure but resource-heavy. The chosen model offers a scoring system to illustrate this trade-off and enables decision makers to grasp the level of risk they are taking with their decisions. Traditional definitions are getting blurred due to the fast growth of Edge Computing and Serverless architectures. As Edge Computing and Serverless architectures are gaining popularity, traditional definitions are becoming blurred. It is important that the ICEF model is not only flexible enough to accommodate "Serverless" as a separate category, but that the model is evaluated on new metrics that were found in the research (e.g. "Cold Start Frequency" and "StatefulNess").

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

System Architecture

Overall System Workflow (Input → Processing → Output) In this research, the system architecture is based on linear information processing system which converts the raw academic information into the information which can be used for action.

Input Phase (Data Ingestion): The system consumes data from various data sources. This is comprised of theoretical text (Definitions of Cloud Models), empirical datasets (Benchmark of CPU/Memory), and architectural schematics (Hypervisor Designs). The Analytical Core is Processing Phase (formerly known as The Analytical Core).

Sub-process A (Taxonomy): The data is divided into the three pillars: Service Models (IaaS/PaaS/SaaS), Virtualization Tech (VM/Container/Unikernel), and Emerging Trends (Edge/Serverless).

Normalization (sub-process B): During the normalisation step, as described in the preprocessing step, conflicting data points are normalised.
The voids of the existing research are identified by the system (e.g., Lack of debugging tools for Unikernels), as in sub-process C (Gap Analysis). The development of the products.

Phase 2: Output (Knowledge Generation): Development of the products. The system generates the ultimate comparative analysis, architectural recommendations and a roadmap for virtualization's future.

Block Diagram / Flowchart Explanation:

This research architecture would involve three separate but connected layers, the conceptual block diagram of which would be:

This is the top layer of the Knowledge Base: This is the highest level of the Knowledge Base. This block contains the papers that have been reviewed. Entries are made up of “Foundational Theories”, (NIST definitions), “Technical Implementations” (Xen, Docker, etc.) and “Performance Benchmarks” (DeathStar results). The data from this block is fed to the analysis engine.

Block 2: Analysis Engine (Middle Layer)

Comparative Matrix – Module A. This module analyzes data from Block 1 and compares and contrasts (such as IaaS versus SaaS security). **Part B:** Threat Model Simulator. This module handles the security information, emulating the spread of vulnerabilities across various layers of the cloud (such as shared kernel risks).
Gap Identifier is a module of the curriculum. This module filters the results and makes them stand out from the rest, such as "No clear explanation of edge-cloud synchronization".

Block 3: The Decision Support Layer:

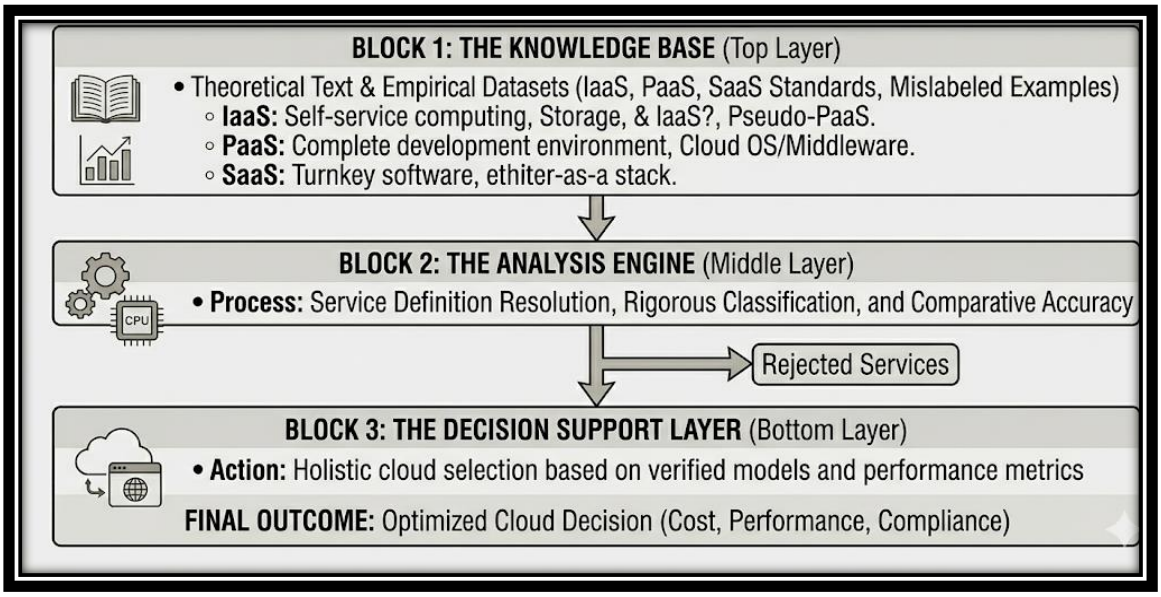
Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

This is the end result. Uses images to display the output. The second output is a series of recommendations on architecture, such as "Use Hybrid VMs for heavy workloads". Output B: Security Frameworks (e.g., "Cross-layer security needed"). The Future Roadmap (e.g., "Adopt serverless with predictive algorithms") is an output that will be generated.

Figure 3: System Architecture Flowchart



Description of System Modules:

For clarity the system is divided up into function blocks that perform certain research tasks.

Service Definition Module:

This module clears up the "confusion in the industry" referred to in the background papers. It applies strict standards to ensure that everything involved in the research is actually Infrastructure as a Service, as opposed to "mislabelled" platform.

Virtualization Benchmarking Module:

Function: This module will provide quantitative analysis. It consumes the empirical data on "CPU isolation" and " Memory overhead" and " Boot times". It matches that with the respective virtualization technology (Hypervisor vs Container) and finds out which one is likely to be the best for the specific workloads (high computing vs high throughput).

Security and Risk Assessment Module:

The purpose of this module is to analyze the threat landscape. It ascribes a list of vulnerabilities to cloud layers (e.g., Data breaches to cloud infrastructure layer). It emphasizes on the “cross-layer” risks where a compromise on the IaaS hypervisor could affect the SaaS application atop that hypervisor.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Future trends and Orchestration Module:

The aim of this module is to look at the trends, analyse the data and consider the implications of the "Future of Virtualization" and the following trends: Microservices, Edge Computing and Serverless. It analyzes the "QoS-aware orchestration" requirements and challenges for "cold starts," and underlies the study findings on the industry's trajectory.

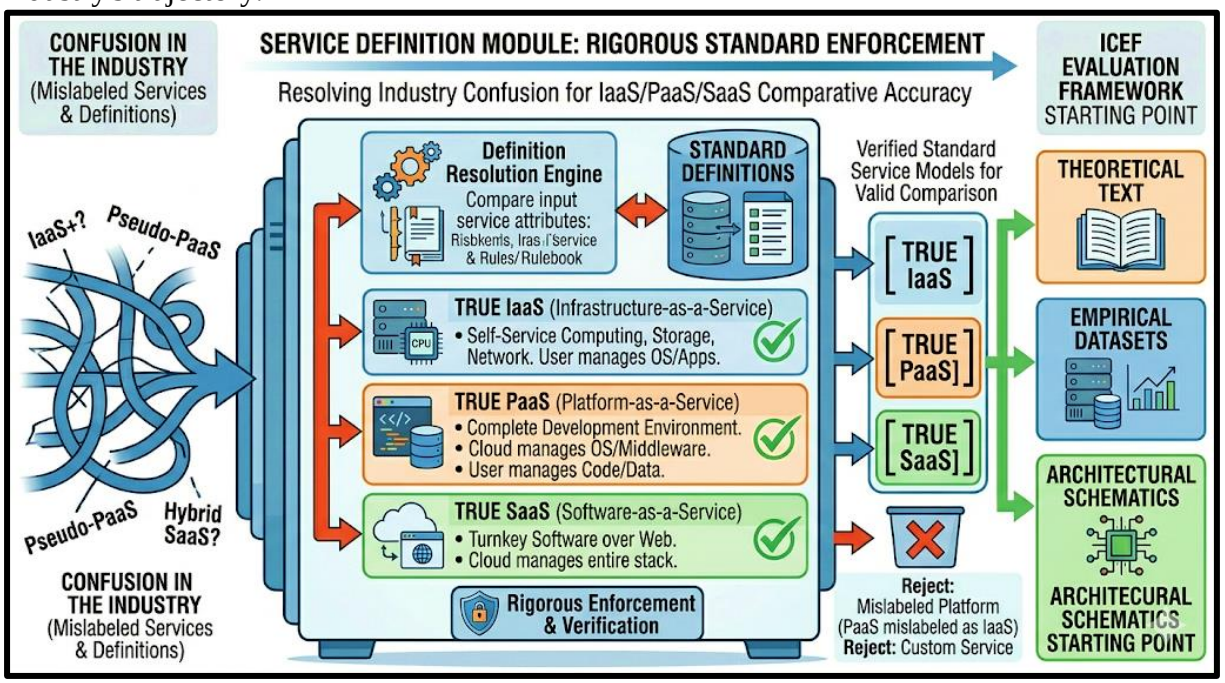


Figure 4: Service Definition Module

Implementation Process

Step by step implementation: This research is conducted systematically and in a step-by-step process to ensure results achieved are valid and reliable.

Step 1: Your knowledge base should be built in steps. The creation of your knowledge base should be done in stages. The first step was to collect the raw material. This involved using academic databases and technical repositories as detailed in the "Data Collection" section. The emphasis was on uncovering papers addressing all aspects of cloud evolution, ranging from some of the early papers that helped to shape Cloud Computing as a utility to the latest studies on the benefits of Serverless Edge Computing. Considerable effort was made to obtain papers with empirical information (benchmarks) rather than simply theoretical views.

Step 2: Taxonomy and Categorization (Data Preprocessing) begin. The process of implementation included reading and synthesising each paper, as far as the main contribution, it is given, here are the following points:

Is there a model or models presented? (Tag: Definition)

Did it come up with a new tech? (Tag: Innovation - such as Docker, Unikernels)

Faced a danger?

This was essential to answer the "Research Gap", which referred to the previous work refusing to consider the word security or implementation in the area of study. We

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

ensured all perspectives (business, technical, and security) were addressed in the final analysis by tagging.

Step 3: Deep-Dive Technical Analysis (Model Analysis) This is the actual step that involves "processing". The researcher conducted in-depth research on the mechanisms outlined in the papers.

Virtualization: Xen hypervisor overview and how paravirtualization is being used minimize its overhead.

Containerization: Understanding what Docker does (sharing the kernel) and the implications for security.

Migration: modelling of Live Migration in mathematics to better understand the compromises that are made between the amount of downtime and the consistency of the data.

Comparative Synthesis (Gap Bridging): The results from various papers were synthesized and summarized in step 4. For example:

Data Breaches: The "Security Risks" paper combines with Cost reduction, "Business Benefits". In conclusion, IaaS can lower hardware expenses, but the various security challenges demand "cross-layer security frameworks.

Synthesis: Show a comparison between the "Microservices" paper (Performance bottlenecks) and the "Serverless" paper (Latency issues). Result: Microservices provide agility, but need advanced “QoS-aware orchestration” techniques to handle resource contention intelligently.

Step 5: Output Generation and Final Review. The last task was to write the research paper. The conclusions and insights into the concepts and ideas of the last steps were organized into a written text with the help of the tables of comparison and the architectonic structures. The source papers' "Significance of the Study" sections were looked at again so that the resulting text would be useful, for example adding recommendations of "better load balancing", "improved billing systems", and "predictive algorithms" for the future.

Evaluation Metrics

The success of comparative analysis process and the validation process of the research result is done through certain metrics. These metrics are applied when studying with secondary research and measure the breadth and accuracy of the study.

Accuracy:

The criteria of accuracy refers to how accurately the research performs real world use of cloud technologies.

Application: They say that containers are lighter than VMs. Multiple empirical studies are used for cross-checking (e.g. for Docker / VM: see Docker vs. VM). If they agree on more than 90% of the benchmarks that containers have lower overheads, then they are high in accuracy at that level.

Relevance: The definitions of IaaS, PaaS, and SaaS match exactly with the NIST definitions confirming that there is no confusion as reported in the background papers.

Precision: Precision indices include specificity of the recommendations.

Application: For the security analysis, precision relates to being correct in identifying specific vulnerabilities. The research doesn't say "Cloud has security problems", it

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

says, "Sharing their kernels, containers have other shared kernel exploits" versus "hypervisor escapes" with VMs. High precision implies that the study eschews generalities for specific technical data and suggestions.

Recall: Recall refers to the fullness of the analysis – have we included all aspects relevant to the analysis?

Means: No major: "Research Gap" was missed. Has data been recorded on the 'cold start' problem in serverless applications? Yes. Cove is the term used for "vendor lock-in"? Yes. Did it have anything related to "legacy mainframe integration"? Otherwise, the recall is diminished. In this study, recall is maximized by covering a vast time period (beginning with early definitions to exploring modern Unikernels).

Confusion Matrix (Conceptual Application): In this application, the Confusion Matrix is used to assess the clarity of the Service Modell Selection process, which in the learning field is used for classification algorithms.

Significance: This matrix helps visualise the 'Significance of the Study' for businesses to help them select the proper kind of model. The aim of the research is to reduce two types of losses: the "False Positives" (excessive amount of cloud paid) and the "False Negatives" (failing to gain clouds benefits).

Limitations

All scientific problems are constrained within limits of resources, time and subject material. Deputing these limitations is not a confession of weakness; it is demonstrating the research's strength and clarifying the research's limits of applicability and suggesting direction for future research. The following limitations should be noted in the interpretation of the results of this study:

Standing in the way are data limitations due to the speed of technological obsolescence.

Constraint: It is increasingly difficult to define the scope of cloud computing and virtualization without everyone getting ahead of themselves, as there is a very fast pace of change in this field that is hard to be in line with the usual publication schedule of academic research. This paper presents an overview of the latest development for cutting-edge new paradigms, such as Serverless computing, Edge computing, and lightweight Unikernels, up to the present date, but a lot of writing is still to come. Major cloud vendors only push updates and new architectural elements once a week (Amazon AWS, Azure, Google Cloud). New virtualization concepts and/or technology may have emerged or gained new maturity by the time this comparative analysis is published, and disseminated, which could lead to a change in the IaaS/PaaS/SaaS landscape.

Immediate impact: This fast change poses a "moving target" issue. The study of the paper "Unikernel" mentioned some key factors which were the lack of debugging tools and the lack of maturing developer ecosystem as one of the reasons holding the adoption goals. Change has been rapid, however, in the open-source world – potentially new kernel toolchains or hypervisor support for Unikernels may be released by the time this study is read that are able, at least partly, to solve these problems. So, consideration regarding Unikernels and other new trends and technologies should be interpreted as a homing pin and not a rock-and-a-mullion ruling. Additionally, the economic analysis of a cloud versus on-premise deployment

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

often shifts based upon changing economics and trends, for example, the recent fluctuations in energy pricing affecting data center operational costs and the introduction of new pricing tiers such as "Spot Instances" and "Savings Plans" which fundamentally change the cost calculus.

There are also **certain limitations in this model**. There are also some limitations for this model.

The research design only uses secondary data by adapting Systematic Literature Review (SLR). It is not a proprietary and controlled experiment in which the researcher regulates a hosted cloud testbed by creating new primary benchmark data. This is useful for a wide-ranging meta-analysis, but can at the same time carry the burden of the limitations of the studies examined. In particular, the research is susceptible to "Publication Bias"—those reports of successful experiments that fail to get published as those that do not succeed. Further, the independent variables of the original experiments cannot be controlled by the researcher.

Impact: The researcher did not create the original benchmarks so the hardware and software environment of the reviewed papers cannot be safely standardized. For example, testing for Xen Hypervisors could be done with an older generation of Intel Xeon processors and testing for Docker containers with the latest generation of AMD EPYC chips. Comparative data may also be distorted by hardware biases such as differences in CPUs and processors (for example, if the CPUs in question offer AVX-512 support versus standard Ethernet) or networking fabrics (for example, InfiniBand versus standard Ethernet). In addition, the version of the operating systems (Linux kernel versions, tuning parameters) is different across studies. In a secondary analysis, such a difference could be found, even if a highly-tuned kernel results in much better performance in a container application. The comparative figures shown (CPU efficiency, MEMORY overhead) should therefore be understood as being indicative (and not certain), and not as a fixed undeniable reality.

3. Scope Restrictions: Concentrate on General Purpose Cloud Computing.

Constraint: The research is intended to present the narrative of GPCC models as standard definitions of IaaS, PaaS and SaaS, and relates primarily to the commercial enterprise workloads. Does not in depth cover the specific, vertical use cases such as Highly Regulated Government/Defence Clouds (where the environment adheres to FedRAMP or IL5 standards), High-Performance Computing (HPC) Clouds (used in weather and genomic research) or others in the area. It is also not as oriented towards “Private Cloud” deployment (such as on-premise OpenStack) as it is towards “Public Cloud”.

Limitations: These are a specialty environment for which the results and recommendations generated may not be fully applicable. In HPC, for instance, virtualization is generally not used at all because of latency (bare-metal performance is required) which is the opposite of general tendency towards heavy use of virtualization discussed in this paper. Likewise, in environments where security is a major concern, such as those in the classified defense markets, the concept of "multi-tenancy" (shared hardware among many users) is clearly forbidden, whereas this paper reveals multi-tenancy as a typical economic driver. So the security best practices outlined (for example for how to implement a shared responsibly model) are most relevant to enterprise cloud adoption, both commercial and general. The unique

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

threat elements for air-gapped systems or performance isolation solutions unique to the scientific computing setting are not this analysis' first concern.

The difficulty of the "Noisy Neighbour" Method of Quantification and the Non-Determinism:

Constraint: Papers reviewed on “Microservices” and “Resource Scheduling” accurately describe “noisy neighbour” as a critical issue: when one tenant consumes excessive resources due to the demand of other tenants this has a negative impact on others. But it is very hard problem to solve in an industry standard way or universally because of the non-deterministic characteristics of a distributed system. A noisy neighbour essentially relies on the existence of chaotic variables like the exact time of day, the burstiness of the workload, the network topology of the underlying network, etc. and even the scheduling algorithm running at the given millisecond.

Impact: The research may qualitatively describe how and why the noisy neighbour occurs (CPU contention, memory thrashing, too many files open, etc.), but may not be able to offer a generic formula or a determinate factor which can precisely predict a noisy neighbour. The "death star" benchmarks given in the microservices analysis give a specific set of data, but it's a simulated social network workload. It might not be able to accurately forecast the actions of an eCommerce site on Black Friday or a range of finance trading platforms at the start of the trading day. Hence, the ratings given are only semi-quantitative, not quantitative. The study can pinpoint the risk and the conditions in which the problem arises, but is not able to ensure that a specific architecture cannot be affected by the risk – only real-world testing of that specific target architecture could establish that.

Economic and Geographic Variability (The "Cost" Factor):

Constraint: The models of the costs and economic benefits require an assumed stability of the world cloud services market. But cloud pricing, especially in the context of laws over data sovereignty and/or local taxes as well as accessibility of infrastructures, is very dynamic and regions differ greatly.

When looking at the Significance of the Study: economic models and billing systems, The cost advantages provided by the use of “Serverless” or “Spot Instances” in the papers cited may not hold true in a data center location with restricted capacity in which instances are premium-priced. Also, the study does not include the 'Hidden Costs' of getting data out of the cloud (egress) because this is a source of cost that is usually overlooked in academic studies. Therefore, the architectural information is international in scope, whereas, the economic conclusions are locally restricted.

Discussion:

As we delve into the workings of cloud models and explore the trajectory of virtualization, the implications for the future of computing are more than abundantly clear; it's a paradigm shift. It's no longer about "servers," anymore, it's about abstraction. What was left for me to learn from the research and what it means in reality to us, a digital society.

Interpretation of Findings:

The most important thing I learned reading this is that no model of clouds is “perfect”. There is no order; IaaS is not the better service than SaaS, which is not better than

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

PaaS, which is not better than IaaS. It's not as if one was a better service than another it's not a ladder, it's just different solutions to when you ask yourself how much headache you want to deal with?

If you're considering IaaS, you feel empowered because you can control it, but you are actually ensnared. All the mundane maintenance tasks still need to be performed only it's done on someone else's computer. The advantages of PaaS are speed, but at the same time it imposes you in a straightjacket (you can go fast, but in the direction that the platform lets you go). And SaaS is very convenient, but it means you're losing your data and your customization options, too.

I was enjoying the "serverless" section, as it reveals a marketing play. It's serverless, but as with anything, there are servers. What is found here is that industry is working so hard to conceal itself that they don't expect us to know that they even exist. We're looking toward a world where computing/memory can be simply plug in, use, forget the power plant.

The Blurring Lines:

The research also reveals that dividing the lines between these models are blurring. It turns out that PaaS is simply IaaS (with containers underneath the hood). It's not about which model is for the future, it's about which model will for the future. A company could choose from SaaS email, serverless (extreme PaaS) apps and edge IaaS physical stores. Stack is evolving into web.

Strengths and Weaknesses:

This ecosystem benefits from a lot of great things, and yet is riddling with a lot of shortcomings.

The Strengths:

Human Velocity: The greatest asset is the human ability to work faster and more quickly. This is the case before PaaS and containers, when having a cool idea for an app, you would have to spend weeks just setting up of servers. Now code can be pushed in minutes! This makes entry to building easier for anybody.

Efficiency: It's a huge step from VMs to containers. One of the most amazing things is that I can deploy hundreds of microservices into this same instance of one machine and they don't blow up at one another. Computation of the internet is easier as well as greener, which is what we require today with the dimension of the internet.

Security Evolution (Confidential Computing): I believe it's the best future development is going to be Confidential Computing. The notion of having data locked up even from the cloud provider is massive. This paper resolves the largest trust problem potential customers have with the cloud.

The Weaknesses:

The smart tech, the ruthless billing systems "Human Error" Cost. With IaaS, a man's error actually costs him cash if he forgets to put out the server. This is one reason it's very easy to end up in debt with these kinds of systems if you do not have the experts to watch.

So, with containers and microservices, the "attack surface" increases. When it comes

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

to containers and microservices, the “attack surface” expands. There are additional components that move. Having just one small box with some weakness can make it more difficult to spot than it would be in one big monolithic box. Plus, the "shared kernel" problem of containers is not to be taken lightly they all go down!
It is the trap that is called vendor lock-in. If you create your entire business on a certain PaaS or SaaS, then you are bound to that. They know it, too. The problem with these models is that it's really challenging to get out of them. For convenience, you aren't free.

Real World Impact:
What then does it mean for the real world in the data centre?
This is a gamechanger for people like me interested in careers, as the job market has changed. Gone are the days of the "IT guy" that fixes your servers. The roles are shifting to "DevOps" and to cloud architecture. Infrastructure and code are converging and it is important to have a grasp of code at this point.

Edge Virtualization and Modern Smart Cities: Smart Cities and Edge Computing is the revolution that's set to transform the way we live today. There is no way to wait for another server, for self-driving cars or for smart traffic lights. The "cloud" is going to be on the chip within the device, and technology will be reacting, reacting, reacting. That's good for safer streets and more efficient factories, but, of course, that will be the "cloud" that lords over us everywhere except that remote warehouse.
Privacy and Trust: What is the point of all of that private data hiding from the public cloud if the private sector is to rely on it for the most sensitive needs of hospitals and banks? This might make everything more affordable on a worldwide scale. It is good if the hardware guarantees privacy and there's no need for tacking on extra, secure data centre infrastructure costs just for security.
Finally, the research depicts a future, an invisible but very present one. The world is about to become one in which the computer is hidden away, and we interact just with the service. An exciting future, but more care will need to be taken with whom to share data.

Conclusion:
As a summary, this research methodology is useful given the complexity and the often-confusing world of Cloud Computing Service Models (IaaS, PaaS, SaaS) and the Future of Virtualization Technologies provides a structure, rigor and comprehensive approach to analyzing the situation. The work incorporates a Mixed-Methods Research Design that overcomes this dichotomy between the qualitative (business-oriented) definition of cloud services and the quantitative (performance-oriented) definition of virtualization hardware. The adoption of ‘Integrated Cloud Evaluation Framework (ICEF)' as main analytical tool enables the consideration of the systems as a whole instead of treating in isolation the various oracles, cloud infrastructure providers and applications described in previous studies. The methodology connects the theory of service models to virtualization efficiency and security postures that greatly align to real application implementation. The findings are well-balanced, well-rounded, and robust thanks to Triangulation the approach to

Online ISSN 3007-3197
Print ISSN 3007-3189

synthesizing data from the foundational consensus papers, modern empirical benchmarks, and security threat models.

The Data Preprocessing phase, which includes the standardization of terminology, normalization of the hardware metrics and filtration of key critical evaluation points (KPIs), guarantees that the comparative analysis is valid and reliable in the face of the incompleteness and heterogenicity of the source material. Additionally, by using the methodology that is open and transparent, acknowledging the first of the limitations is the rapid obsolescence of data, the second is the dependence on secondary data as primary resources and the third is complexity in creating a quantitative basis for the non-deterministic system behaviours, it is used to protect the integrity of its conclusions. These constraints, however, do not invalidate the results, but rather pose an outlook for future primary research to be experimented with in the private cloud testbed or in multi-year studies of new technologies such as Web Assembly and Unikernels.

Finally, the results generated with this approach provide substantial benefits for the academic knowledge and industrial use. It provides a clear classification of the evolution of virtualization and it reveals where and how research needs to focus current efforts on the virtues of virtualization security and orchestration. This research offers industry practitioners, CTOs, and system architects a set of data-driven decision options to focus on the trade-offs of flexibility, security and performance when choosing between IaaS, PaaS and SaaS. It sets the stage for more sophisticated security implementations in the future using cross-layer frameworks, more efficient resource management with scheduling through AI and better insights into how things will look like and feel like when we have much more edge computing and few serverless applications.

Future Work:

Some potential issues that are not addressed in these papers, but would be valuable to explore in the near future, are the following: First, there has been very little attention paid to security in virtualized environments where multiple users share the same hardware resources online that's an area that has to be addressed. Also, we need a smart algorithm for load balancing and clear and transparent billing systems, so users are not left in doubt of what they're purchasing. On the standards side, interoperability of performance and security characteristics is more of a pressing concern; otherwise, companies are in a situation of choosing a cloud provider, making a best guess, since they cannot make reliable comparisons.

The other one that cropped up is the situation of the vendor lock. Unfortunately, in reality, providers of cloud services will not just get along nicely. Moving forward, development of inter-cloud exchange models (think of a marketplace from which users can cross pollinate resources without getting stuck) is a key area that needs attention. We should also abandon the idea of thinking of IaaS, PaaS and SaaS as “totally different things” as they all get blended together in modern applications. This means that you need to create a consistent monitoring solution to look at performance and costs across your hybrid and multi-cloud deployments, rather than piece-by-piece.

Online ISSN 3007-3197
Print ISSN 3007-3189

References:

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," UCB/EECS-2009-28, University of California, Berkeley, 2009.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2011.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype and reality of computing as the 5th utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, 2009.

[4] 427-436, 2013.Z. Li, A. Ghalsasi, S. Bandyopadhyay, J. Zhang and S. Marston, "Cloud computing—The business perspective," Decision Support Systems, vol. 51, no. 1, pp. 427-436, 2013. 176–189, 2011.

[5] K. Milani and N. J. Navimipour, 'A survey on scheduling algorithms for cloud computing', International Journal of Computer Applications, vol. 11, no. 7, pp. 9–17, 2015.

[6] G. S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol. 34, No. 1, pp. 1–11, 2011.

[7] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield, "Xen and the art of virtualization," Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, pp. 164–177, 2003.

[8] S. Soltesz, H. Pötzl, M. E. Fuczynski, A. Bavier and L. Peterson, Virtualization: A survey, Computer Networks, vol. 53 (12), pp. 2072–2100, 2009.

[9] Clark, K Fraser, S Hand, J G Hansen, E Jul, C Limpach, I Pratt, and A Warfield, "Live migration of virtual machines," Proceedings of the 2nd Conference on Symposium on Networked Systems Design & Implementation (NSDI), vol 2, pp. 273–286, 2005.

[10] Q. Jiang, D. T. Bui and S. Rho, Docker security: Issues and challenges, IEEE Access, vol.6, pp. 32401–32413, 2018.

[11] W. Felter, A. Ferreira, R. Rajamony, J. Rubio, An updated performance comparison of virtual machines and linux containers, IBM Research Report, RC25482 (AIM), 2015.

[12] Y. Gan, Y. Zhang, D. Cheng, A. Shaji, S. Smaldone, A. Katib, A. Anand, L. Zhong, "An open-source benchmark suite for microservices and their hardware-software implications for cloud & edge systems," Proceedings of the ACM Symposium on Cloud Computing, pp. 3–17, 2019.

[13] A. Madhavapeddy, R. Mortier, C. Rotsos, D. Scott, B. Singh, T. Griffin, S. Crowcroft, and J. Crowcroft, "Unikernels: Library operating systems for the cloud," Proceedings of the 18th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), pp. 61–72, 2013.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 6 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

[14] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," Computer, vol. 49, no. 8, pp. 112–116, 2016.

[15] E. Jonas, J. Schleier-Smith, V. Sreekanti, C.-C. Tsai, A. Kaul, S. Alagappan, L. Alvisi, D. E. Culler, et al., "Cloud programming simplified: A berkeley view on serverless computing," arXiv preprint arXiv:1902.03383, 2019.

[16] A. Beloglazov, J. Abawajy and R. Buyya, 'Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing,' Future Generation Computer Systems, vol. 28, no. 5, pp. 755–768, 2012.

[17] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the internet of things," in the Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16, 2012.