RESEARCH ARTICLE OPEN ACCESS

A Comparative Study of Cloud Security in Public vs. Private Cloud Environments

Mohammed Asif Sawant
(MCA department, Sinhgad Institute of Business Administration and Research (SIBAR), Pune, India
Email: mohmmedasifsawant93@gmail.com)

Abstract:

Cloud computing is now used by almost every company because it gives flexibility, cost saving, and quick setup. But security is a major issue especially when chosen either public and private clouds. Public clouds are cheap and grow easily nut they are less safe. Private clouds are safe but it cost more. This research tries to find the balance solution by looking at hybrid setup and helps to find out which model give better balanced effective solution. Findings indicate that with correct security tools and policies both models can be easily depending on organizational needs.

Keywords — **cloud computing, public cloud, private cloud, hybrid cloud, cloud security**, **shared responsibility**

I. INTRODUCTION

In recent years cloud computing has fully changed how companies handle their IT work. Companies can rent tech from big companies. Now companies can save money and start projects fast.

But with all these benefits security has become a major issue. Companies worry about cloud security because it is risky. The main question that comes up is which model gives better security — public cloud or private cloud.

• Public cloud is shared space managed by someone else.

•Private cloud is used by only one organization and gives more control but at a higher cost.

• This research helps organizations select the best cloud option by making difference between security and risks.

A. Statement of the Problem

Many companies are still confused about which cloud model gives better security. Provider and customer both handle the cloud security.

Many organizations think the provider handles everything but that is not true. The provider only secures the main infrastructure. The user must take care of their data, apps and access settings. because of this misunderstanding, many setups have mistakes that open doors to attacks.

Most of the cloud data breaches happen due to wrong settings. These breaches cost companies about $4.24 million each. As businesses use more clouds, the risk increases.

This clearly shows the need for a simple and practical way to handle cloud security that fits properly with the chosen model.

B. Objectives of the Research

- We need to learn about cloud security and how it will be.
- We will learn about cloud problems like data leaks and rule issues and privacy issues.
- To compare security strengths and weak points of public and private cloud models.
- To give practical ideas for improving safety in both cloud setups.

C. Significance of the Study

This research helps managers and IT teams understand public and private clouds better. It helps companies pick the right cloud for their data.

This helps organizations secure their business. The study also explains how hybrid clouds and new tools like zero trust and cloud security posture management (CSPM) can strengthen protection without adding too much cost.

II. RELATED WORK

Past studies haved studied cloud computing and cloud security in unique ways where they focused on ways cloud help business growth and risks like loss of privacy and data leaks. This part shows what was already found and how it connects to this study.

A. Studies on Cloud Adoption

•Some studies found that

o Small companies like public cloud because it is cheap and easy.

o Big companies like hospitals and banks prefer private cloud for better security and control.

•Some studies also mentioned hybrid cloud but they did not explain clearly how its security works in real use.

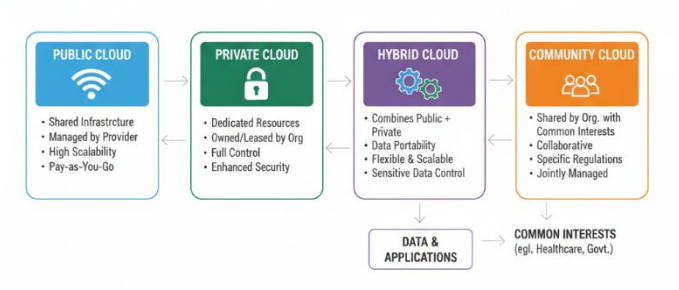

Fig. 1: Cloud deployment models

B. Security Challenges in Cloud Systems

- Many studies discussed that cloud systems are open to risks like hacking, data leaks and wrong configuration.
- Modern Cloud Security Concepts (gupta & mehta 2024) explained that most problems happen because of human mistakes such as wrong access rules or weak passwords.
- Most of these papers agree that proper training and monitoring tools can reduce such incidents.

C. Shared Responsibility Model

- Documents from AWS Security Guide and Microsoft Azure Documentation clearly describe the shared responsibility model.
- Many companies still misunderstand this and think the provider handles everything which causes setup errors.
- Researchers suggest that better guidelines and awareness programs can make this concept clear for all cloud users.

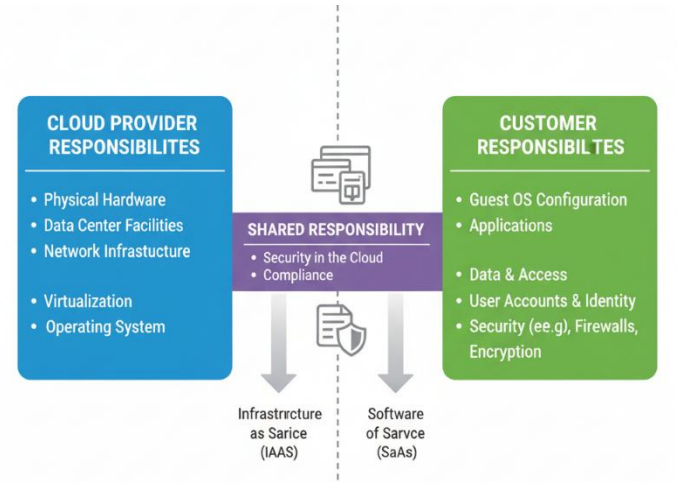

Fig. 2: Shared Responsibility M

D. Use of Security Tools

• Tools like Cloud Security Posture Management (CSPM) are used to find wrong configurations and fix them automatically.
• Other idea can be Zero Trust Architecture in it nothing is trusted automatically.
• AI-based monitoring tools are also becoming popular for detecting abnormal activity in real time
• These tools are very effective but not all companies use them because of high cost or less knowledge.

E. Compliance and Legal Studies

• Some papers focused on rules like GDPR and HIPAA that affect cloud usage.
• These rules require companies to protect personal and health data properly.
• Private cloud is often preferred for compliance, but hybrid cloud can also work if set up correctly.
• Researchers suggest that cloud systems must be designed with legal rules in mind.

F. Gaps in Existing Research

• Most previous studies focused only on public or only on private cloud models, not comparing both together in detail.
• Studies that mention hybrid models often skip the practical use of tools like CSPM and Zero Trust in those environments.
• This study aims to fill these gaps by comparing how each model manages security and by suggesting a balanced method that fits different business needs.

III. METHODOLOGY

This research is done using a structured review method and simple content analysis no new data was collected through experiments or surveys.
Instead, information was studied from academic papers, industry reports, and official documents of cloud providers like aws, azure, and google cloud the main aim was to understand how different cloud models work in terms of security, cost, compliance, and how easy or hard they are to manage.

A. Research Design

• The study follows a descriptive and comparative approach, using secondary data.
• To check for patterns and risks between different cloud environments.
• A hypothetical case study was used to apply findings in a realistic business scenario.

B. Source Selection Criteria

•Around 30 sources from 2021 to 2025 were studied, including
- o Journal papers and conference articles
- o Whitepapers from aws, azure, and google cloud.
- o Official security and compliance guidelines like GDPR, HIPAA, and NIST CSF.

•Sources were selected for
- o Clear focus on cloud security and deployment models.
- o Discussion on problems like misconfigurations and insider threats.

C. Data Collection Process

•Each selected document was read carefully and main points were written down under these topics
- o Security risks and vulnerabilities.
- o Cost and resource control.
- o Legal compliance and data handling.
- Scalability and ease of operation.

All notes were kept in a spreadsheet to compare what each model does better or worse.

D. Content Analysis Method

• Manual coding was used to group similar points and find repeated themes.
• Every cloud model was checked based on
- o Level of risk and security exposure.
- o How flexible it is for compliance laws.
- o Cost efficiency and ease of management.

• Simple tables were made to show clear comparisons.

E. Case Scenario Development

• A sample company named innovate tech was created to show how results work in real life.
• The company had two major needs.
    o To protect customer data safely.
    o To run a large public website with good performance.
• This setup helped to see how each cloud model handles both security and scalability together.

F. Tool Evaluation Strategy

• The study checked how different security tools work in public, private, and hybrid cloud setups
    o CSPM was studied for finding and fixing wrong settings or misconfigurations
    o Zero trust architecture was seen for controlling user access and reducing insider risks
    o Ai-based monitoring tools were noted for detecting threats in real time
• Each tools usefulness was judged by how easy it is to use, how much it can automate, and how well it fits with other systems.

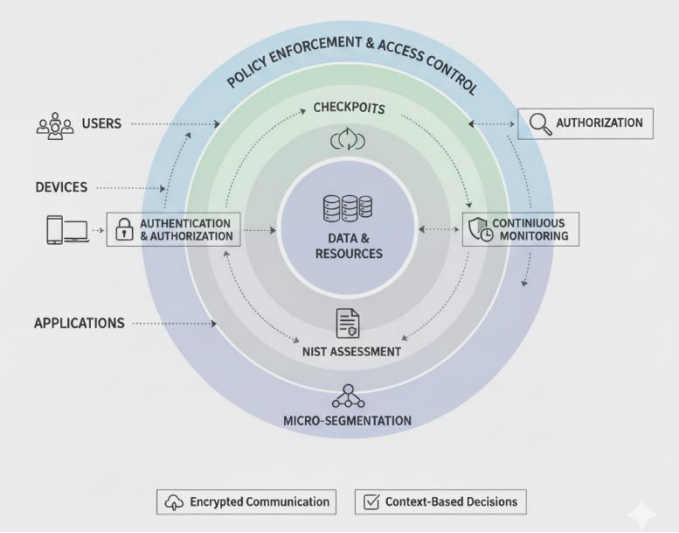

Fig. 3: Zero Trust Architecture (ZTA)

G. Limitations of the Method

• The research is based fully on secondary data and document study, not live testing or attack simulation.
• The case study is only a sample example, so results may not be the same in real company setups.
• Cost details are based on estimates from reports, not actual cloud provider bills.

IV. RESULTS AND ANALYSIS

This section shows the outcomes of comparing public and private cloud environments. The aim is to highlight both strengths and weaknesses and explain how organizations such as innovate tech can use these insights for real business decisions.
The analysis includes examples and structured comparisons from real industry cases.

A. Security Behavior Across Cloud Models

Security is the most critical factor in cloud computing. Public clouds has multiple users where they share the same physical hardware so by this it increases chances of external attacks. Full control and data isolation is done if the users configurations are weak and this offer is given by private cloud.
Overall, public clouds need strict configuration and monitoring, while private clouds need strong internal access control to stay secure.

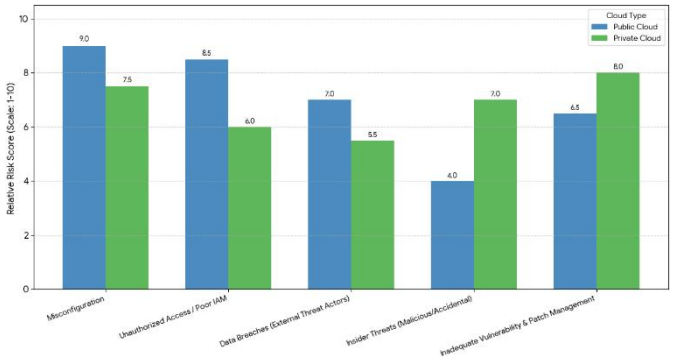

Fig. 4: Comparative security risk

TABLE I
Security Behavior – Public vs. Private Cloud

Security Factor	Public Cloud	Private Cloud
Misconfiguration Risk	High – frequent due to user errors	Medium – fewer users, more controlled
Insider Threat Risk	Low – limited internal access	High – wider insider access
External Attack Surface	Wide – shared infrastructure	Narrow – dedicated environment
Access Control Flexibility	Limited – depends on provider IAM	Full – custom access policies possible
Encryption Control	Provider-managed	Organization-managed
Audit and Monitoring	Basic logs; advanced tools cost extra	Full visibility and custom monitoring

Interpretation:

• From the comparison, public clouds are more open to misconfigurations, which can lead to data leaks or exposure.

• However, they face lower insider threat risks because internal employees have limited access to infrastructure.

• Private clouds give complete control and isolation making it safe.

• But since more internal staff manage the system, insider threats become a bigger concern.

B. Cost and Resource Efficiency

• Cost is a key factor in choosing between cloud models.

• Companies using public clouds only pay for what they use this helps very much in such way

o This lowers upfront spending and helps scale resources easily.

o For example, netflix uses aws public cloud to increase capacity during busy hours and reduce it later, saving huge costs.

• Private clouds require buying and maintaining servers, which makes them expensive to start but stable in long-term budgeting.

o Banking and healthcare like this cost model because it's predictable and safe.

TABLE II
Cost Comparison – Public vs. Private Cloud

Cost Factor	Public Cloud	Private Cloud
Upfront Investment	Low – pay-as-you-go	High – hardware and maintenance costs
Operational Costs	Variable – depends on usage	Fixed – predictable monthly costs
Scalability	High – elastic provisioning	Limited – depends on in-house servers
Resource Utilization	Elastic – no idle resources	Fixed – idle servers during low demand
Cost Control Tools	Cloud-native dashboards and alerts	Manual or custom tracking systems

Interpretation:
• Public cloud helps avoid wasting resources because you only pay for what you use.
• But if usage increases suddenly and is not tracked, costs can rise quickly.
• Private cloud helps to control the costs and makes budget easy.
• However, it can waste money if servers are not fully used.

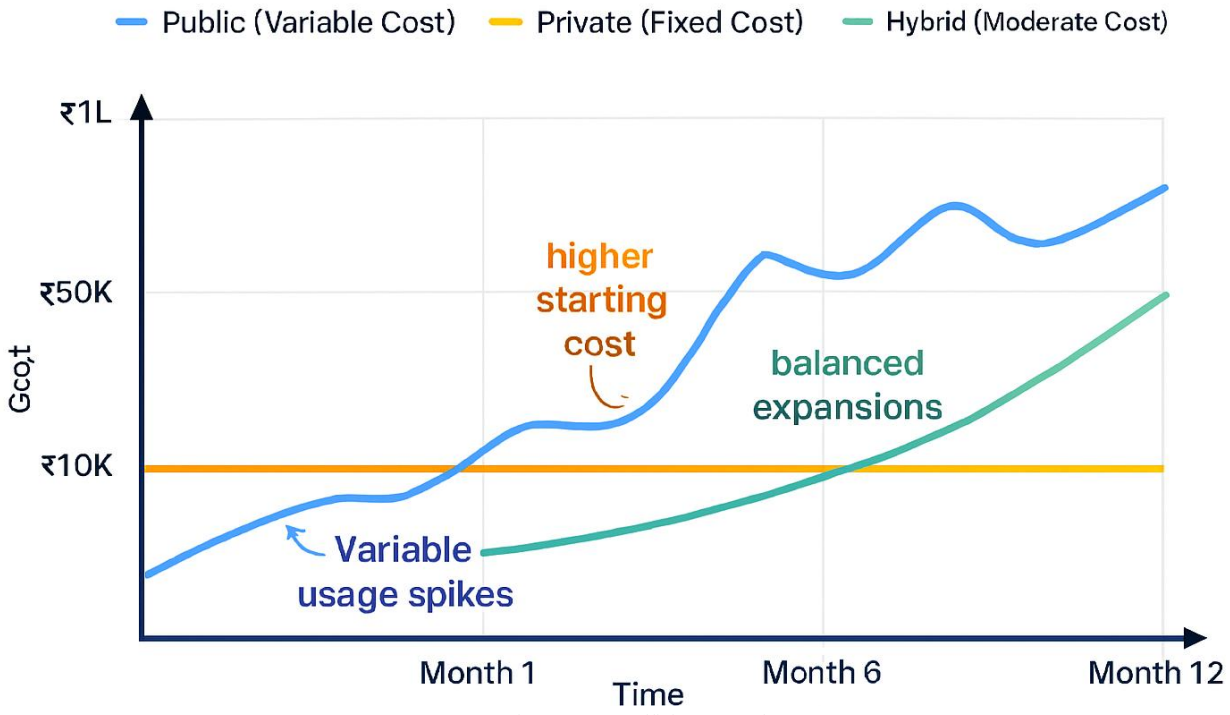

Figure 5: Cost efficiency trends

C. Compliance and Legal Readiness

• Companies that have sensitive data have to follow the strict rules.
• Private cloud is good for healthcare and banking because it gives more control and better audits.
• It supports laws like HIPAA and GDPR.
• Public cloud can also meet compliance needs using tools like AWS Artifact or Azure Compliance Manager.
• But the company using it must set up everything correctly.
• If settings are wrong, data can be exposed and cause rule violations.

TABLE III
Compliance Readiness – Public vs. Private Cloud

Compliance Factor	Public Cloud	Private Cloud
Data Residency Control	Limited – provider decides region	Full – organization decides location
Audit Support	Moderate – access to provider logs	High – complete access to all logs
Regulatory Flexibility	Low – shared environment restrictions	High – customized for regulations
Encryption Standards	Provider-managed	Organization-defined
Legal Risk Exposure	Higher – shared infrastructure	Lower – isolated and controlled

Interpretation:

• Private cloud is better for industries that need strong compliance, like healthcare or finance.
• But public cloud users can also meet compliance rules if they set configurations correctly and train their staff.

D. Scalability and Performance

• Public cloud is very good at handling sudden high traffic or usage spikes.
• Companies like amazon india and flipkart use it to manage heavy festive season loads.
• Private cloud gives stable and consistent performance.
• But it has limited capacity, so if usage grows suddenly, services can slow down.

TABLE IV
Scalability and Performance – Public vs. Private Cloud

Scalability Factor	Public Cloud	Private Cloud
Traffic Handling	Excellent – elastic scaling	Limited – fixed resources
Performance Consistency	Variable – shared load affects speed	High – dedicated resources only
Load Balancing	Built-in by provider	Manual or custom solutions required
Downtime Risk	Low – backed by SLAs	Depends on internal maintenance
Response Time	Fast – optimized for global reach	Fast – within local network

Interpretation:

• Public cloud is best for scalability and quick growth.
• Private cloud is best for steady and reliable performance.

E. Tool Integration and Automation

• Both cloud types use modern tools for better security and automation.
• Now a days companies uses CSPM and Zero Trust and also AI to monitor cloud security.
• Public cloud provides these tools as built-in options — for example, aws guard duty for threat detection.
• Private cloud needs manual setup or outside tools, but this gives more control and customization.

TABLE V
Tool Integration – Public vs. Private Cloud

Tool Type	Public Cloud	Private Cloud
CSPM (Misconfiguration Fix)	Highly effective, provider-native	Needed but fewer misconfigurations
Zero Trust Architecture	Supported through cloud IAM	Fully customizable implementation
AI Threat Monitoring	Real-time detection at scale	Requires internal integration
Automation Potential	High – APIs and scripts supported	Medium – depends on local IT tools
Response Speed	Fast – automated alerts and actions	Slower – may require manual checks

Interpretation:

• Hybrid cloud setups use tools like automation and ai to manage both public and private systems easily.
• Automation helps reduce errors and saves time in managing complex environments.

F. Summary of Key Insights

1.Public cloud is best for scalability, flexibility, and cost savings, but can face more external attacks and misconfigurations.
2. Private cloud is secure but costly and not very scalable.
3.Hybrid cloud: combines both models and gives a balanced and practical solution for most organizations.
4.Common risk: wrong configurations still cause most cloud security issues.
5. Future trend: automation and zero trust and aslo AI tools will make cloud safer and reduce manual work.

G. Overall Comparative Analysis

• No single cloud model fits all business needs.
• Every cloud model has its good side of view and bad side of view.

TABLE VI
Overall Comparison of Public and Private Cloud Models

Parameter	Public Cloud	Private Cloud	Best Use Case
Security Control	Moderate – depends on provider setup	Strong – full internal control	Private Cloud
Cost Efficiency	Excellent – pay only for usage	Low – high fixed expenses	Public Cloud
Scalability	Very High – automatic resource allocation	Limited – depends on local hardware	Public Cloud
Compliance	Limited – requires careful setup	Strong – easy to meet legal standards	Private Cloud
Performance	Variable under shared load	Consistent and reliable	Private Cloud
Automation Tools	Widely available	Customizable, requires setup	Hybrid Cloud
Maintenance Needs	Low – handled by provider	High – internal IT needed	Public Cloud
Ideal For	Startups, e-commerce, dynamic workloads	Banks, healthcare, government	Hybrid for balance

Interpretation:

• Public cloud is best for startups or online companies that need fast growth and global access at low cost.
• Private cloud is used for banks, hospitals, and government offices that need strict data to be manage and compliance.
• Most modern companies now use a **hybrid cloud** — keeping sensitive data in private servers and using public cloud for scalable apps or websites.
• This hybrid model gives a good balance of security and performance and also flexibility.

V. DISCUSSION

This part explains the results and their connection to real cloud use and aslo including how models work and tools help to manage cost and control and also the complexity.

A. Security Behavior in Cloud Models

• Each cloud type works differently for security.
• **Public cloud** is open and flexible but more likely to face errors or wrong settings.
  o Most breaches happen because users forget to enable encryption or leave data public.
  o Example: in 2023, many amazon s3 users had data leaks because of public access settings.
• **Private cloud** gives full control and reduces outside threats but insider mistakes, like weak passwords or missed updates, can cause problems.
• **Hybrid cloud** mixes public and private clouds to separating sensitive data from regular work and reducing risks but it requires proper management.

B. Role of Security Tools

• Tools are important to keep clouds safe.
• **CSPM** finds and fixes wrong settings automatically — best for public cloud mistakes.
• **zero trust** means "never trust, always verify" every user or device must be checked each time they access data even stolen passwords cant give full access.
• **Ai-based monitoring** keeps watching for strange activity and alerts instantly. Example: microsoft defender for cloud uses ai to catch risky logins early.

• These tools help stop attacks before they cause damage.

C. Cost and Resource Use

• **Public cloud** is cheaper at first and uses pay-as-you-go system good for startups and changing workloads and extra security can increase cost.
• **Private cloud** needs more money at the start for servers and hardware gives full control and steady monthly costs.
• **Hybrid cloud** saves money by keeping important data private and public apps outside this gives both security and cost balance.

D. Complexity and Management

• Hybrid cloud gives flexibility but is harder to manage so teams must control many systems together.
• **Automation tools** help by fixing mistakes, checking security, and sending alerts by the help of cspm can warn if encryption is off and by ai tools can show system health and detect attacks early.
• With training and planning, hybrid setups can be managed easily and safely.

E. Overall View

All cloud model has good and bad points

• **Private cloud** is good for control and following rules but its costly and needs smart people.
• **Private cloud** gives control and compliance but it costs more and needs experts to handle it.
• **Hybrid cloud:** best balanced model with both safety and flexibility.
• Depends on company needs budget and staff skills.
• Zero trust and CSPM and also the AI tools make cloud secure and easy to manage.

VI. *Findings and Suggestions*

This section gives key points and useful advice for companies and developers and also the researchers. It says to turn technical results into clean steps that can help to reduce risk and better cloud security decisions.

A. Key Findings from the Comparative Study

1. Security behavior changes by cloud model
• Public cloud is more open and can face more misconfigurations.
• Most problems happen because users forget to set access control or encryption.
• Private cloud is safer from outside attacks but faces insider risks.
• Hybrid cloud reduces both risks when used properly.
2. Cost depends on usage and planning
• Public cloud is cheap at first and best for startups or changing workloads.
• But cost can go up fast if usage increases or if extra security tools are added.
• Private cloud is costly at the start but gives full control and fixed monthly cost.
• Hybrid cloud helps balance both—important data in private and scalable apps in public.
3. Compliance is easier in private cloud
• Private clouds are better for strict rules like gdpr, hipaa, or banking laws.
• Public clouds can also meet rules but only if users set them up correctly.
• Hybrid cloud gives you the flexibility and control for sensitive data.
4. Security tools are very important
• Tools like **cspm**, **zero trust**, and **ai monitoring** help find and fix risks.
• Public cloud often has built-in tools.
• Private cloud needs manual setup.
• Hybrid cloud gains most from automation because it connects many platforms.
5. Hybrid clouds are hard to manage
• Managing is not easy when public and private cloud are mixed.
• Without automation, mistakes can happen.
• Good tools and training make hybrid setups safe and also it make smooth.

B. Suggestions for Organizations

1. choose cloud based on needs
• Not to pick a cloud type blindly.
• While you select think about data, security, budget, and team skills so u can select the proper cloud.
• Startups can use public cloud.
• Hospitals or banks should use private or hybrid for more control.
2. Train staff on cloud security
• Because of the human error it causes most data leaks.
• Train the employees on the basis of the encryption, access, and security settings.
• Run workshops, audits, and test attacks to have the better awareness.
3. Use automation to avoid errors
• Doing everything manually is risky.
• Use tools that watch and fix things by themselves.
• This helps prevent mistakes and quickens response time.
4. apply zero trust and cspm tools
• zero trust checks every login request.
• cspm keeps scanning for wrong settings and compliance gaps.
• These should be part of every cloud setup, especially hybrid .
5. track and control cloud costs
• Use dashboards and alerts to check spending.
• Remove unused resources and adjust capacity when not needed.
• Hybrid cloud helps balance costs by dividing workloads smartly.

C. Suggestions for Developers and Researchers

1. Build better hybrid support tools
• Build tools that work on all clouds.

• Shared dashboards, real-time alerts, and easy management add this all to build hybrid support tools.

2. Focus on user behavior
• Study how users handle cloud security tools.
• Find out if they understand alerts and act on them.
• Design tools that are simple and user-friendly.
3. Study advanced threats
• Test cloud systems against new attack types like phishing or stolen credentials.
• Run safe simulations to find weak points early.

VII. Conclusion and Future Work

A. Conclusion

• The four areas which are risks, cost, compliance, and security tools are been studied and looked at public vs private cloud security so it will have better use.
• From the findings, no single cloud model is perfect for all organizations.
• There are good and bad points in every model it dependence on the company.

Public Cloud

• For having perfect small businesses public clouds are cheap and flexible.
• They allow quick scaling when demand increases.
• But they face security risks from human errors like bad settings or access control mistakes.
• Most attacks happen because of misconfiguration and weak monitoring.

Private Cloud

• Private clouds give full control over data and system.
• They are best for companies that must follow strict rules like GDPR or HIPAA.
• Needs more money and skilled people.
• Still it need regular checks and internal security to prevent insider threats and leaks.

Hybrid Cloud

• Hybrid clouds mix public and private benefits.
• We keep important things in private cloud and other things in public cloud.
• It makes safer and saves money.
• Managing hybrid clouds is hard, so we need automation and constant monitoring.

Modern Security Tools

• Tools like CSPM, Zero Trust Architecture, and AI threat detection are now necessary.
• They help find wrong settings, control access, and stop attacks early.
• These tools are very useful when using hybrid cloud systems.

B. Future Work

• Future studies should test real users and threats to improve cloud security.
• For better cloud security the future studies should be focused on real world user behavior and also on advanced threat testing.

1. Understanding User Behavior and Awareness
• Many security problems happen because of human mistakes, not just system faults.
• Future research should study how employees and admins use cloud systems in daily work.
• This show how they react to alerts and follow security rules and how they handle private data.
• By knowing this, better training programs and easier security tools can be developed.

2. Conducting Advanced Threat Simulations
• Researchers should perform real attack simulations in a safe test setup.
• This can include password theft, ssl spoofing, api attacks, or combined cyberattacks.
• These tests will show how strong current cloud systems are in real situations.
• They will also help find weak points that need stronger protection.

3. Studying the Trade-off Between Performance and Security
• Shopping sites, banks and hospitals are facing problem with balancing speed and security.
• Systems need to run fast for users but must also stay safe from attacks.
• Even having high traffic or emergencies future research should focus on balancing speed and security.

4. Strengthening Policy Enforcement in Hybrid Models

• Keeping the same security rules in both public and private clouds is still a big challenge.
• Future research can work on new tools or methods that make it easier to apply the same access control, encryption, and compliance checks across all cloud platforms.
• This will help companies manage hybrid setups more safely and easily.

C. Closing Reflection

• Cloud computing has become the base of modern digital life — almost every company depends on it now.
• More data in the cloud means more security matters.
• Providers give tools so users must use them in right way in this way both work together for cloud security.
• Success comes from having the idea of risks, learning and using smart automation.
• Teamwork will make future cloud systems better.

VIII. REFERENCES

[1] E. Ghazaryan, "Comparative Analysis of Cloud Deployment Models: Public, Private, Hybrid, and Multi-Cloud," *International Journal Of Engineering And Computer Science*, 2025.
[2] D. H. Parekh and R. Sridaran, "An Analysis of Security Challenges in Cloud Computing," *International Journal of Advanced Computer Science and Applications*, 2013.
[3] D. Dattawala and T. Singh, "A Comparative Analysis of Cloud-Based Information Security Solutions: Evaluating Risks and Benefits," *International Journal of Engineering Applied Science and Management*, 2024.
[4] M. Lata and V. Kumar, "Cyber security techniques in cloud environment: comparative analysis of public, private and hybrid cloud," *EDPACS*, 2025.
[5] Thales, "2024 Cloud Security Study - Europe and Middle East Edition," Thales Report, 2024
[6] J. Roper, "Cloud Deployment Models - Types, Comparison & Examples," Spacelift Blog, 2024.
[7] A. Kumar, "A Comparison of Security Challenges in Public and Private Clouds," *International Journal of Latest Trends in Engineering and Technology*, 2014.
[8] F. Shirazi, A. Seddighi, and A. Iqbal, "Cloud Computing Security and Privacy: An Empirical Study," *J. Comp. Theo. Nanosci.*, 2017.
[9] SentinelOne, "Private Vs. Public Cloud Security: 10 Key Differences," SentinelOne Blog, 2025.
[10] A. Ismail and E. Siham, "Enhancing Cloud Security: Strategies and Technologies for Protecting Data in Cloud Environments," *International Journal of Applied Mathematics Computational Science and Systems Engineering*, 2024.
[11] M. Kharma and A. Taweel, "Threat Modeling in Cloud Computing - A Literature Review," in *Ubiquitous Security*, Springer, 2023.
[12] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *NIST Special Publication 800-145*, Sep. 2011.
[13] StrongDM, "Public vs. Private Clouds: What's the Difference?," StrongDM Blog, 2024.
[14] CDNetworks, "Public Cloud Security vs Private Cloud Security," CDNetworks Blog, 2024.
[15] Check Point Software, "Top Cloud Security Trends in 2025," Check Point Software Cyber Hub, 2025.
[16] B. B. Sehgal, "How AI Impacts Cloud Security," CrowdStrike Blog, 2025.
[17] H. B. Patel and N. Kansara, "Cloud Computing Deployment Models: A Comparative Study," *International Journal of Innovative Research in Computer Science & Technology*, 2021.
[18] B. Balkin, "NIST Cyber Security Framework – 5 Core Functions Infographic," CalCom Software Blog, 2025.
[19] O. Gierszal and L. Knoll, "Private Cloud vs Public Cloud: How To Choose The Right Cloud Solution," Brainhub Library, 2025.
[20] Shubham, "Private Cloud in 2025: Trends, Technologies, and Best Practices," Cloudian Guide, 2025.
[21] Google Cloud, "What is Zero Trust?," Google Cloud Blog, 2025.
[22] S. Moore, "Cloud Security: Challenges, Solutions, and 6 Critical Best Practices," Exabeam Explainer, 2025.

IX. APPENDIX

A. Tools and Platforms Used

• Research sources used include researchgate, nist, sentinelone, thales, crowdstrike, check point, google cloud, and exabeam.
• aws, azure, google cloud, OpenStack, VMware, and hybrid clouds this all are been studied for having better research.
• security tools referred in the study.
    o Cloud security posture management (cspm) – to find and fix wrong settings.
    o zero trust architecture (zta) – for strict access control.
    o ai-based threat detection – like microsoft defender for cloud, used for real-time monitoring
• Compliance standards included gdpr, hipaa, and the nist cybersecurity framework.
• Deployment cases studied came from e-commerce, healthcare, and finance industries.

B. Observation Parameters

• Security behavior – studied misconfiguration risks, insider threats, and exposure to outside attacks.
• As per the study it was seen that the costs like setup, running, scalability, and resource usage.
• Compliance readiness – looked at data location, audit support, and flexibility for legal rules.

• The study looked at the tools how they get integrate and automate.
• Complexity management – studied policy handling, cross-platform visibility, and training needs.