International Journal of Advanced Engineering and Technology
www.allengineeringjournal.com
ISSN: 2456-7655
Received: 07-03-2026, Accepted: 07-04-2026, Published: 22-04-2026
Volume 10, Issue 2, 2026, Page No. 44-46

Cloud security in the AI era: Technical threats, user behavior, and case studies

Shubhangi Pawar, Sawant Apurva Ramesh, Sapkal Ganesh Bhanudas, Adul das Km, Yadav Rambharosh Manoj Kumar
Department of Computer Science, Pillai College of Arts, Commerce and Science, Panvel, Navi Mumbai, Maharashtra, India

Abstract
Cloud computing has become the foundation of modern digital infrastructure, enabling organizations to store data, run applications, and deliver services efficiently through remote servers. The widespread adoption of cloud services has significantly improved scalability, flexibility, and cost efficiency for businesses. However, the rapid growth of cloud environments has also increased security risks. Many organizations rely on multi-cloud or hybrid cloud architectures, which increases system complexity and expands the potential attack surface for cybercriminals.
At the same time, Artificial Intelligence (AI) is transforming the field of cybersecurity. Security teams use AI and machine learning to detect threats, identify unusual activities, and respond to attacks faster than traditional security systems. However, attackers are also leveraging AI technologies to automate hacking activities such as phishing attacks, password cracking, and credential theft [1]. As a result, the cybersecurity landscape has become more dynamic and complex.
The purpose of this study is to analyze the major technical threats present in cloud environments and examine the role of human behavior in cloud security incidents. The research adopts a descriptive methodology based on secondary data collected from cybersecurity reports, academic publications, and industry surveys. The findings indicate that most cloud security incidents occur due to misconfigurations, weak authentication mechanisms, stolen credentials, and lack of user awareness. Human error remains one of the most significant causes of data breaches in cloud systems [2].
The study concludes that effective cloud security requires a combination of advanced technical controls, AI-based threat detection systems, and responsible user practices. Organizations must strengthen identity protection, enforce security policies, and implement continuous monitoring to reduce risks in the modern AI-driven cloud environment.

Keywords: Cloud computing, cybersecurity, artificial intelligence, machine learning, cloud security risks, multi-cloud architecture, hybrid cloud, threat detection

Introduction

Cloud computing has become an essential component of modern information technology infrastructure. Organizations across industries use cloud platforms for data storage, application hosting, collaboration, and digital service delivery. Popular cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform provide scalable and flexible computing resources that allow organizations to operate efficiently without maintaining physical infrastructure.
Despite its advantages, cloud computing introduces several security concerns. Sensitive organizational and personal data stored in cloud environments can become attractive targets for cyber attackers. Unauthorized access, data breaches, and service disruptions can result in financial losses, reputational damage, and legal consequences for organizations.
Another major development influencing cloud security is the rapid advancement of Artificial Intelligence (AI). AI technologies are widely used in cybersecurity for tasks such as intrusion detection, threat intelligence analysis, anomaly detection, and automated incident response. Machine learning algorithms can analyze large volumes of network data and identify suspicious activities much faster than traditional rule-based systems.
However, AI technologies also introduce new security challenges. Cyber attackers are increasingly using AI tools to generate automated phishing campaigns, deepfake content, intelligent malware, and sophisticated password-cracking techniques. This has made modern cyberattacks more scalable, targeted, and difficult to detect.
In addition to technical vulnerabilities, human behavior plays a critical role in cloud security incidents. Poor password management, failure to enable security features, accidental data exposure, and lack of cybersecurity awareness often lead to security breaches. Therefore, cloud security must address both technical risks and human-related vulnerabilities.

Literature Review

Several studies highlight the growing security challenges associated with cloud computing environments. Researchers have identified common cloud vulnerabilities such as misconfigured storage services, insecure APIs, insufficient access control policies, and improper identity management. Misconfigured cloud resources, such as publicly accessible storage buckets, have been responsible for many high-profile data breaches in recent years [3].
Another major concern in cloud security is identity and access management (IAM). Weak authentication systems and stolen credentials are among the leading causes of cloud security incidents. Attackers frequently exploit compromised user accounts to gain unauthorized access to sensitive cloud resources.
Human behavior also contributes significantly to cloud security failures. Studies show that many users adopt weak passwords, reuse credentials across multiple platforms, and fail to activate multi-factor authentication (MFA). In addition, employees may fall victim to phishing attacks or social engineering techniques, which allow attackers to obtain login credentials or sensitive information.

Artificial Intelligence has emerged as a powerful tool in cybersecurity defense. AI-based security solutions can analyze large volumes of network traffic, detect unusual behavior, and respond to potential threats automatically. However, researchers also warn that cybercriminals are using AI to develop more sophisticated attack methods such as AI-generated phishing emails, deepfake impersonation attacks, and automated vulnerability scanning tools.
As a result, modern cloud security strategies must combine advanced technical defenses, AI-driven monitoring systems, and strong security awareness programs to protect organizational assets.

Purpose of the Study
The purpose of this research is to analyze the evolving security challenges of cloud computing in the era of Artificial Intelligence. As organizations increasingly rely on cloud infrastructure and AI-based technologies, new risks such as data breaches, AI model manipulation, and unauthorized access continue to emerge.
This research aims to:

- Identify major technical threats affecting cloud environments integrated with AI technologies.
- Examine how user behavior and human factors contribute to cloud security vulnerabilities.
- Analyze real-world case studies of cloud security breaches and incidents.
- Evaluate current cloud security practices and recommend improved strategies for protecting cloud infrastructure and AI systems.

The study aims to provide practical insights that can help organizations strengthen their cloud security frameworks and minimize risks associated with AI-driven technologies.

Scope of the Research
This research focuses on the intersection of cloud computing, artificial intelligence, and cybersecurity. The scope includes:

- Analysis of technical security threats in cloud environments such as data leakage, insecure APIs, AI model attacks, and cloud misconfigurations.
- Examination of user behavior factors, including poor password practices, lack of cybersecurity awareness, and improper access control management.
- Study of selected real-world case studies involving cloud security breaches in organizations using AI technologies.
- Review of existing cloud security frameworks, policies, and mitigation strategies used by organizations.

However, the study is limited to secondary data sources and publicly available case studies. It does not involve direct penetration testing or experimentation on live cloud systems.

Research Gap
Although numerous studies discuss cloud security and others focus on AI-related cybersecurity threats, limited research examines the combined impact of AI technologies and human behavior on cloud security risks.
Existing research often:

- Focuses mainly on technical vulnerabilities while ignoring the influence of human behavior.
- Examines AI security and cloud security separately instead of analyzing their interaction.
- Provides theoretical discussions but lacks real-world case study analysis.

Therefore, there is a need for research that integrates technical risks, behavioral factors, and practical security incidents to provide a more comprehensive understanding of cloud security challenges in the AI era.

Overview of Methodology
This study adopts a qualitative and analytical research methodology to examine cloud security challenges in the context of Artificial Intelligence.
The research primarily relies on secondary data sources, including:

- Academic research papers
- Cybersecurity industry reports
- Government publications
- Documented case studies of cloud security incidents

The research process begins with a literature review to identify existing knowledge about cloud computing security, AI-based threats, and user behavior in cybersecurity.
Next, the study analyzes human behavior factors such as weak password practices, lack of awareness, and improper access control. These factors help explain why many security breaches occur despite the availability of advanced security technologies.
The research also examines real-world case studies of cloud security incidents to identify common patterns, root causes, and organizational impacts.
Finally, the collected findings are evaluated to identify major security challenges and recommend effective strategies for improving cloud security in AI-driven environments.

Data Analysis and Interpretation
The analysis indicates that many users remain unaware of fundamental cloud security practices. Basic protection measures such as strong password management, multi-factor authentication, and secure configuration settings are often neglected.
Organizations also face increasing threats from credential theft, phishing attacks, and misconfigured cloud services. These vulnerabilities allow attackers to gain unauthorized access to sensitive cloud resources.
Furthermore, the study finds that AI technologies are increasing the speed and scale of cyber attacks. Automated attack tools powered by AI can perform large-scale password attacks, phishing campaigns, and vulnerability scanning much faster than traditional methods.
These findings highlight the importance of continuous monitoring, proactive threat detection, and improved cybersecurity awareness programs.

Conclusion
Cloud computing has become a critical technology for modern organizations, but it also introduces new security risks. This study shows that many cloud security incidents occur due to a combination of technical vulnerabilities and human error.
Artificial Intelligence plays a dual role in cybersecurity. While AI helps organizations detect threats faster and

automate security responses, attackers are also using AI to develop more advanced and scalable cyberattack techniques. Therefore, effective cloud security cannot rely solely on technological solutions. Organizations must combine advanced security technologies, strong authentication mechanisms, proper cloud configuration practices, and continuous user awareness training.

Implementing modern security strategies such as the Zero Trust security model, identity-based access control, and AI-driven monitoring systems can significantly reduce cloud security risks. By adopting a proactive and comprehensive security approach, organizations can ensure safer cloud operations in the rapidly evolving AI-driven digital environment.

Limitations of the Study

This research has several limitations that should be considered when interpreting the findings. First, the study relies primarily on secondary data sources, including academic papers, cybersecurity reports, and publicly available case studies. As a result, the research depends on previously published information rather than direct experimentation or primary data collection.

Second, the study focuses mainly on documented cloud security incidents, which means that some security breaches or vulnerabilities that organizations keep confidential may not be included in the analysis. Many companies do not publicly disclose security failures due to reputational and legal concerns.

Third, the rapid evolution of cloud technologies and artificial intelligence may cause some findings to become outdated over time. Cybersecurity threats are constantly evolving, and new attack techniques and defense mechanisms continue to emerge.

Finally, the research does not include practical penetration testing or technical experimentation on live cloud systems, which could provide deeper insights into real-time vulnerabilities and attack patterns.

Despite these limitations, the study provides valuable insights into the major technical and human-related factors influencing cloud security risks in the AI-driven digital environment.

Future Research Directions

Future research can expand this study in several important areas. First, researchers can explore real-time security monitoring systems powered by artificial intelligence, which can automatically detect and respond to cyber threats in cloud environments.

Second, further studies can examine the development of explainable AI (XAI) techniques in cybersecurity. Improving the transparency of AI-based security systems will help organizations better understand how threat detection models make decisions and improve trust in automated security solutions.

Third, future research can focus on behavioral cybersecurity, analyzing how employee awareness, training programs, and organizational culture influence cloud security practices.

Another important research direction is the evaluation of Zero Trust security architectures, which emphasize continuous verification of user identities and strict access control within cloud systems.

Finally, more empirical research and real-world case studies should be conducted to understand how organizations implement cloud security strategies and how effective these strategies are in preventing cyber attacks.

These research directions can contribute to the development of stronger and more adaptive cloud security frameworks for the evolving digital ecosystem.

References

1. Behl A, Behl K. Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press, 2017.
2. Stallings W, Brown L. Computer Security: Principles and Practice (4th ed.). Pearson, 2018.
3. Mell P, Grance T. The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2011.