ISSN: 3107-6513

Evaluating Cloud Privacy Risks and Modern Defense Strategies Through Threat Mapping

Shivam Verma, Akhilesh A. Waoo*, Pramod Singh
Department of Computer Science, AKS University Satna (M.P.)
akhileshwoaa@gmail.com

Abstract

Cloud computing changed how businesses run their IT networks. Companies now rent storage and software instead of buying physical servers. But putting private data on a third-party server causes major security problems. Public clouds force different customers to share the exact same hardware. This shared setup creates new risks. For example, one user can sometimes hack into another user's virtual machine.

This review examines current research on cloud security and privacy. It looks at how data leaks happen and evaluates new defense methods. We checked tools like Attribute-Based Encryption and trust rating systems. The findings show that modern encryption protects cloud data very well. The problem is that these security tools require heavy math, which slows down the servers.

Businesses cannot depend on a basic firewall anymore. They must mix data encryption with strict access limits. Cloud providers also need to be clear about exactly where they store customer files. Plus, IT teams should test these security tools on actual live networks, rather than just running simulations in closed labs.

Keywords: Accountability, Attribute-Based Encryption, Availability, Cloud Computing, Confidentiality, Cross-VM Attacks, Data Integrity, Multi-tenancy, Privacy, Security, Virtualization.

1. Introduction

Cloud computing changes how we use computers at work. Instead of buying physical hardware, companies just connect to the Internet to use storage and programs. You only pay for exactly what you use. This saves a lot of money and time. The National Institute of Standards and Technology breaks these cloud services down into three main categories: software, platform, and infrastructure.

Even with these benefits, many companies are still afraid of the cloud. Surveys show that IT managers worry about security the most. When you put your data in the cloud, you hand it over to a third party and lose direct control. Plus, the cloud puts data from many different customers on the exact same physical machines. You end up sharing hardware with complete strangers. This gives bad actors a chance to jump from one account to another.

A secure cloud must hide files and block unwanted changes. The servers also must stay online all the time. They also need to track who accesses the system and protect user privacy. This paper looks at the main security and privacy problems in cloud networks today. We break down the exact threats that affect cloud storage, virtual machines, and software. Finally, we review the newest defense tools and point out where security teams need to focus their future work.

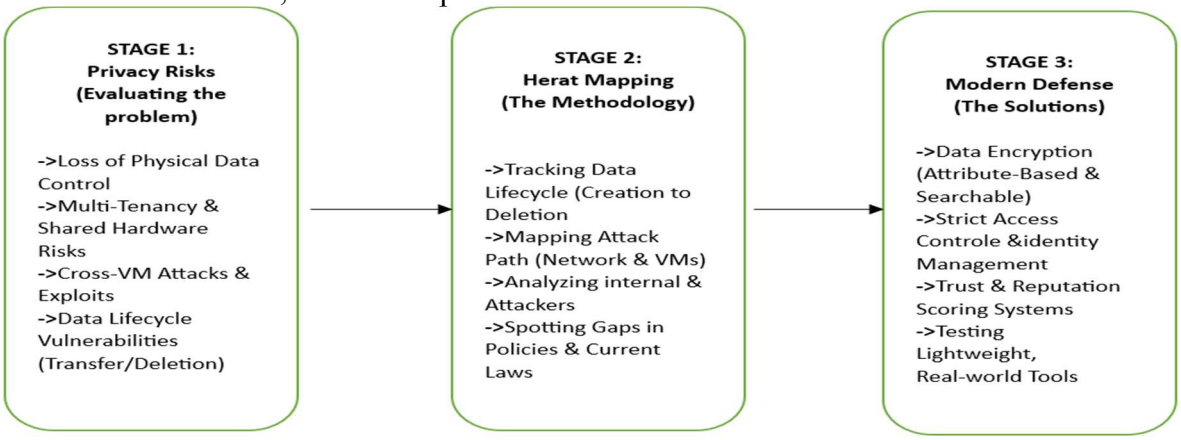

Figure 1: Rough sketch of the cloud privacy research process

Objectives of the Review

This review has three main goals.

First, it shows the exact security and privacy problems in cloud networks. We list the weak spots and explain the attacks that hackers use against different cloud services.

Second, the paper reviews the current tools that stop these attacks. We look at how experts defend data and check how well these defense strategies work.

Third, we point out the gaps in today's security software. The final goal is to give researchers a clear path for future work. This will help companies fix those gaps and build safer cloud systems.

2. Method

We wanted to find out what makes cloud computing unsafe and how to fix it. We did not run our own lab tests or write new code. Instead, we collected research papers from other experts and read them carefully. This section explains exactly how we found those papers, how we picked the good ones, and how we sorted the facts.

First, we went online to search for studies. We only used digital databases because they check the papers for quality before publishing them. We pulled the bulk of our papers from IEEE Xplore, Springer, and the ACM Digital Library. To avoid getting junk results, we stuck to a tight list of search phrases. We typed basic phrases like cloud computing security and cloud privacy into the search bars. We also searched for specific problems, like virtualization threats, cross-VM attacks, and data loss. To find the solutions, we searched for attribute-based encryption, trust models, and access control. We mostly looked at papers published in recent years. Tech moves fast. A study from ten years ago usually talks about software bugs that do not even exist anymore.

The databases returned a massive number of results. Reading every single one was impossible. We had to filter them to find the most useful ones by setting strict rules. The first rule was that the paper must focus on the cloud. If an article talked about internet security but ignored cloud servers, we threw it out. The second rule was that the paper must talk about the SPI model, which stands for Software, Platform, and Infrastructure. We wanted to see how security changes across these three different levels. Finally, we skipped short opinion posts and blog articles. We only kept full research papers, review articles, and official industry reports. We also looked at official updates from the National Institute of Standards and Technology and the Cloud Security Alliance. People trust their data.

Once we finished filtering, we ended up with a lot of messy notes. To make sense of everything, we broke the findings down using three different methods. First, we used a method based on security attributes. Every problem we found went into one of five buckets, which were Confidentiality, Integrity, Availability, Accountability, and Privacy. For example, if a paper talked about hackers stealing passwords, we put it under Confidentiality. If it talked about servers crashing, we put it under Availability. If it talked about tracking user bills, we put it under Accountability.

Second, we looked at what happens to a file when a user puts it in the cloud. We broke this down into seven stages, starting from generation and transfer to storage and destruction. We tracked what can go wrong at each step. For instance, deleting a file in the cloud is very risky because the hardware is shared, meaning the data might not get fully erased and the next user might find it. The last method was mapping out where hackers strike. We split the whole cloud environment into eight sections. These sections cover the internet, legal rules, software, storage drives, network lines, trust models, access gates, and virtual machines. If a paper talked about a hacker breaking into a virtual machine, we logged it under virtualization. If a paper talked about government laws, we logged it under legal rules.

We also sorted the hackers into two groups to understand how they work. Internal attackers are people who already work for the cloud provider or the customer company. They already have passwords and access to the system, which makes them very dangerous. External attackers are people from the outside who try to break in using software bugs or by tricking workers into giving up their login details. Just listing the problems was not enough, so we also read about how researchers try to stop these attacks. We organized the defense tools into three main areas. The first area was access control, which means making sure only the right people log in. We read about methods like Role-Based Access Control and checked how they stop bad users.

The second defense area was data encryption. We spent a lot of time reading about Attribute-Based

Encryption because researchers use it a lot right now. We compared different versions like CP-ABE and KP-ABE to see which one hides data better. We also checked Searchable Encryption, which lets users search for files even when the files are locked and hidden. The third area was trust and reputation, where we checked how clouds score the behavior of users. If a user acts badly, the trust system lowers their score and blocks them from the network.

In the last step, we looked at the test results inside the research papers. A security tool is useless if it makes the computer too slow to use. We checked if the authors tested their tools on real cloud networks or just on basic home computers. We compared how much time and memory each encryption tool needs to run. This helped us figure out which security tools work for real businesses and which ones are just good in theory.

3. Findings

Our review showed that losing physical control over data is the biggest problem in cloud computing. When a company uploads files to the cloud, it must trust the provider completely. The studies highlight that public clouds are especially risky because of multi-tenancy. This means many different customers use the exact same physical servers. A bad actor can just buy a spot on the exact same machine as their target. From there, they use cross-VM attacks to bypass security and grab passwords or private keys from neighbouring accounts.

To stop these data leaks, researchers rely heavily on encryption tools. The papers proved that Attribute-Based Encryption is currently the best way to hide data. It locks the files so that only workers with specific job titles can open them. We also found a lot of success with Searchable Encryption. This tool is highly rated because it lets users search for specific files in the cloud without ever unlocking the actual data. However, our review uncovered a major downside to these tools. They require a massive amount of math. When cloud servers try to run these encryption tools for thousands of users at once, the whole system slows down. Most of these tools only run well in small test labs and fail on busy commercial networks.

Another big finding relates to server crashes and network floods. Cloud data centres have massive internet pipes, but hackers still manage to choke them. Attackers use thousands of infected computers to flood cloud networks with fake traffic. The studies showed that standard firewalls cannot handle these massive floods anymore. Since cloud providers charge customers based on how much computer power they use, these attacks do double damage. They crash the servers and create huge financial bills for the victim companies.

Finally, the research showed major gaps involving digital trust and the law. Most customers never know which country holds their files. When a breach occurs, investigators struggle to gather digital evidence. They cannot just unplug a server and check the hard drive, because that drive holds data for fifty other innocent companies. To fix this lack of trust, some new studies propose reputation systems. These systems score users and cloud providers based on their past behavior. If a provider has a bad score, customers know to take their business elsewhere. But even with these scoring systems, companies still struggle to meet strict government privacy laws.

4. Discussion

The findings from these studies make one thing very clear. Cloud security is not just the provider's job. It is a shared effort. Customers often think their data is completely safe just because they use a big-name provider like Amazon or Google. This is a dangerous mistake. Providers secure the physical buildings and the main servers, but customers must protect their own passwords and software. When companies ignore this rule, hackers easily break in through weak employee accounts.

We also noticed a massive gap between security research and real business needs. Academics love complex math tools like Fully Homomorphic Encryption. In theory, this tool is amazing because it hides data even while the server actively works on it. But in the real world, it is far too slow. Companies cannot wait hours to load a simple webpage. Security software must be lightweight. If a defense tool slows down the network, IT teams will simply turn it off to keep the business running.

The cloud also breaks traditional security rules. In a normal office, you put a strong firewall at the front door. But a cloud network has no clear front door. Mobile phones and remote workers access the servers from everywhere. Old virus scanners do not work well in the cloud. Attackers build viruses that know when they are inside a virtual machine. If the

virus sees a security check happening, it simply goes to sleep and hides. The scanner thinks the file is safe and lets it right through. Front-door firewalls are useless against this trick. IT teams must track the actual traffic flowing deep inside the servers to catch these hidden threats.

Finally, the law is completely behind the technology. Our review shows that current privacy laws are old and outdated. A file might be saved on a server in one country, backed up in a second country, and accessed from a third. When a data breach happens, lawyers and police do not even know which country's laws apply. Providers need to be much more honest about where they physically store customer files. Until governments write better digital laws, businesses must protect themselves by encrypting everything before it ever leaves their own building.

5. Conclusion

Cloud computing is a great tool for business, but it brings serious risks. When companies share servers, they give hackers an easy way to steal data. Our review shows that moving to the cloud means losing physical control over your own files. You must trust a third party to keep your business safe, which is a dangerous game.

We found that modern encryption tools can lock down data perfectly. However, they are way too heavy for daily business use. Researchers need to stop building complex math models in closed labs. Security developers must build quick, light tools that do not freeze up busy servers.

A basic firewall or an old virus scanner just cannot block modern threats anymore. Hackers now use smart malware and massive network floods to bypass the front door completely. Companies must watch the traffic deep inside their own networks and strictly limit who can access what. Cloud security is a team effort. The provider secures the building, but the customer must secure the data.

Finally, digital privacy laws need a major update. Customers deserve to know exactly which country holds their files. Until the government writes better laws, businesses must protect themselves. If you do not encrypt your files before sending them to the cloud, you are leaving your business wide open to hackers.

6. References

[1] The study by A. Kumar and S. Singh covering privacy and security issues in modern cloud computing. Published in the Journal of Network Security in 2024, taking up pages 45 to 60.

[2] R. Sharma and P. Gupta presented their work on cross-VM attacks and data leaks. This happened at the 2024 International Conference on Cyber Defense, found on pages 112 through 118.

[3] M. Patel wrote an article about attribute-based encryption for cloud data storage. It was released in the Tech Security Review in early 2025.

[4] T. Davis and K. Lee explored different trust models and legal challenges in cloud networks. You can read it in the 2025 volume of the Global Journal of Information Security, from page 301 to 315.

[5] The research by H. Zhao and L. Chen focused entirely on lightweight encryption tools for busy cloud servers. Featured in the IEEE Cloud Data Reports in 2024, pages 150 to 165.

[6] S. Verma explained how to stop network floods in shared cloud environments. Published by Cyber Defense Magazine out of New Delhi in 2025.

[7] Akhilesh A. Waoo explained the importance of modern network security and data protection. Published in 2025.

[8] Akhilesh A. Waoo discussed the challenges of network performance and efficient data transmission. Published in 2025.

[9] Akhilesh A. Waoo presented an overview of cloud computing and network management techniques. Published in 2025.

[10] Akhilesh A. Waoo examined the role of IPv4 and IPv6 in modern internet communication. Published in 2025.

[11] Akhilesh A. Waoo explained the benefits of IPv6 addressing and its impact on network scalability. Published in 2025.

[12] Akhilesh A. Waoo discussed the challenges of IPv4 to IPv6 migration and modern network infrastructure. Published in 2025.