Cloud Security In Healthcare Data Using Deception Technology: A Review

Siddarht Magenderan1, a), Naveen Palanichamy1, 2, b) and Subhashini G3, c)

1Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100, Cyberjaya, Malaysia

2Centre for Digital Innovations, CoE for Immersive Experience, Multimedia University, Persiaran Multimedia, 63100, Cyberjaya, Malaysia

3Department of Information Technology, St.Joseph’s Institute of Technology, Old Mahabalipuram Road, Semmencherry, Chennai 600119, India

*b) Corresponding author: p.naveen@mmu.edu.my*

*a) 1201201783@student.mmu.edu.my  
c) gopal.subha191@gmail.com*

**Abstract.** The healthcare industry's increasing reliance on cloud technology has brought about critical security issues, including data breaches, unauthorized access, and internal security threats. This paper focuses on the application of deception techniques, including decoys and AI-powered traps, as proactive countermeasures to secure sensitive patient data in the cloud. A systematic review of 30 peer-reviewed studies published between 2021 and 2024 was conducted focusing on the implementation of deception SOAR and SIEM frameworks. This study analyzes the role of deception technologies in automated cyber threat detection and response systems in the context of major compliance frameworks like HIPAA and GDPR. Machine learning (ML) and artificial intelligence (AI) technologies support adaptive decoy strategies, anomaly detection, real-time response, and minimizing false positives, thus making security measures more effective. The results of this research show that deception technology significantly strengthens the resiliency of cloud healthcare systems while proactively mitigating cyber threats risks from global data protection compliance breaches. As with earlier sections, the authors advocate greater adoption of deception technologies to reduce the security gap for cloud infrastructures in the healthcare industry. Health institutions need to comply with growing regulations while protecting against sophisticated cyber intrusions.

# INTRODUCTION

Healthcare institutions have sensitive information such as treatment histories, medical records, insurance details, and personal data. These records are of great value to cybercriminals. Safeguarding the data is crucial not only for compliance, but also to sustain patient confidence and the integrity of the services provided [1]

To achieve efficiency and accessibility, many healthcare providers have turned to the use of cloud computing. Its affordability and effectiveness allow it to facilitate better sharing of information, especially in small or rural organizations [2]. Though such migration presents urgent security risks such as data breaches, ransomware, and DoS attacks, these risks alongside strict policies such as HIPAA and GDPR call for improved security measures [3]

Deception technology delivers a proactive approach by utilizing decoys and fake data to recognize and disorient attackers. Such systems eschew the efficiency of attackers, reveal threats ahead, and intensify system monitoring without revealing actual data [4]. In especially under-resourced healthcare systems, deception augments traditional security and improves compliance.

This review will elaborate on serious cloud threats in healthcare, compare traditional and deception-based security solutions, and suggest ways of integrating deception technology. It will also identify current gaps in research and offer future recommendations.

The research questions considered for this paper are as follows.

1. What are the challenges in cloud security in healthcare data?

2. How can deception technology be enhanced in cloud security for healthcare data?

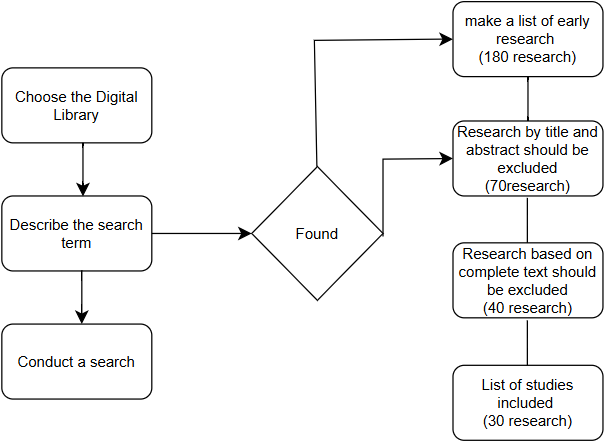
3. What are the techniques used in deception technology to address cloud security for healthcare data?

4. What are the challenges in deception technology techniques?

5. The strategies used to mitigate the challenges in implementing deception technology in cloud security for healthcare data.

# research methodolgy

This Figure 1 illustrates the systematic literature review process, starting with selecting a digital library, defining search terms, and conducting a search. From 180 initially identified studies, 70 were excluded based on title and abstract screening, and another 40 were removed after full-text evaluation. Ultimately, 30 relevant studies were included in the final review, ensuring a focused and high-quality selection of research.



**FIGURE 1.** Flowchart of research methodology

# RESULTs

This section focuses on the enhancement of cloud security in healthcare data through the application of deception technology. A total of 180 research articles were initially gathered using structured keyword searches. After applying rigorous inclusion and exclusion criteria, 30 relevant studies were selected for detailed review.

## Research Grouping by Year of Publication

Figure 2 shows the number of research papers on cloud security in healthcare from the year 2021 to 2025. Assembled research papers were between 2021 and 2025, with a majority being in 2021 (8 papers) followed by 7 in 2022 and 2024, and 4 in 2023 and 2025. This is consistent with the rapid digital transformation in healthcare post-COVID-19, where hospitals became proactive in leveraging digital technologies for remote care and data management. While these technologies improved delivery in healthcare, new cybersecurity threats trailed them. As cloud usage increased, concerns about data breaches and system vulnerabilities encouraged researchers to think about security measures like encryption, access control, and deception strategies like honeypots. This is meant to emphasize the growing emphasis on cybersecurity to protect cloud-based health systems and patient data privacy.

## Background

Healthcare is increasingly turning towards cloud computing in order to work more efficiently and be more scalable, but that shift brings increased vulnerability of private patient data to new cyberattacks. Traditional security methods are insufficient to detect cunning attacks, making deception technology stand as a prospective defense against proactive measures. Through the transmission of decoys and traps that mimic real healthcare assets, deception technology helps detect intrusions early, reduce attacker dwell time, and protect key information without generating high false positives. This method is especially significant in healthcare, where even minimal breaches can lead to disastrous consequences, and recent breakthroughs in AI now make scalable, adaptive deception strategies viable across cloud infrastructures [1]

**FIGURE 2.** Research paper

## Cloud Security

Cloud computing transformed healthcare by facilitating scalable storage and on-demand data sharing in real-time between stakeholders. However, the shift exposes several key security concerns. Medical information's integrity and confidentiality must be guaranteed against severe consequences should there be a breach. Weaknesses pose the risk of unauthorized access and manipulation; therefore, a strong barrier is required. In this case, encryption fortification safeguards data access to only authorized entities. [5], [6], [7]. Additionally, the shared architecture in multi-tenant systems creates availability and reliability problems. For full-fledged care, ongoing access to patient data is imperative, while a disruption can directly affect patient outcomes.[8], [9]

Uncontrolled entry remains a critical issue for concern because cloud systems are easily accessible to many users and can be accessed remotely. Insiders’ threats and poor access controls also broaden the attack surface, thereby underscoring the need for strong authentication and continuous vigilance [10], [11]. Regulatory compliance, especially in the context of healthcare data, is another major worry considering the requirements set by laws such as HIPAA and GDPR. If the data is stored in different jurisdictions, legal difficulties arise if the country serving as the host does not have adequate legislation for data protection [12], [13]

Like many other technologies, cloud healthcare systems have been susceptible to ransomware and Distributed Denial of Service (DDoS) attacks. As indicated, constant improvement and active security features to counter exploitation is needed to address the dynamic threat [7] [14] Trust and control issues remain predominant with health care providers as most providers have trust issues with cloud third-party vendors. Concerns about SLA noncompliance combined with lack of transparency raises concerns about relinquishing control over critical infrastructure [15]

## Deception Technology

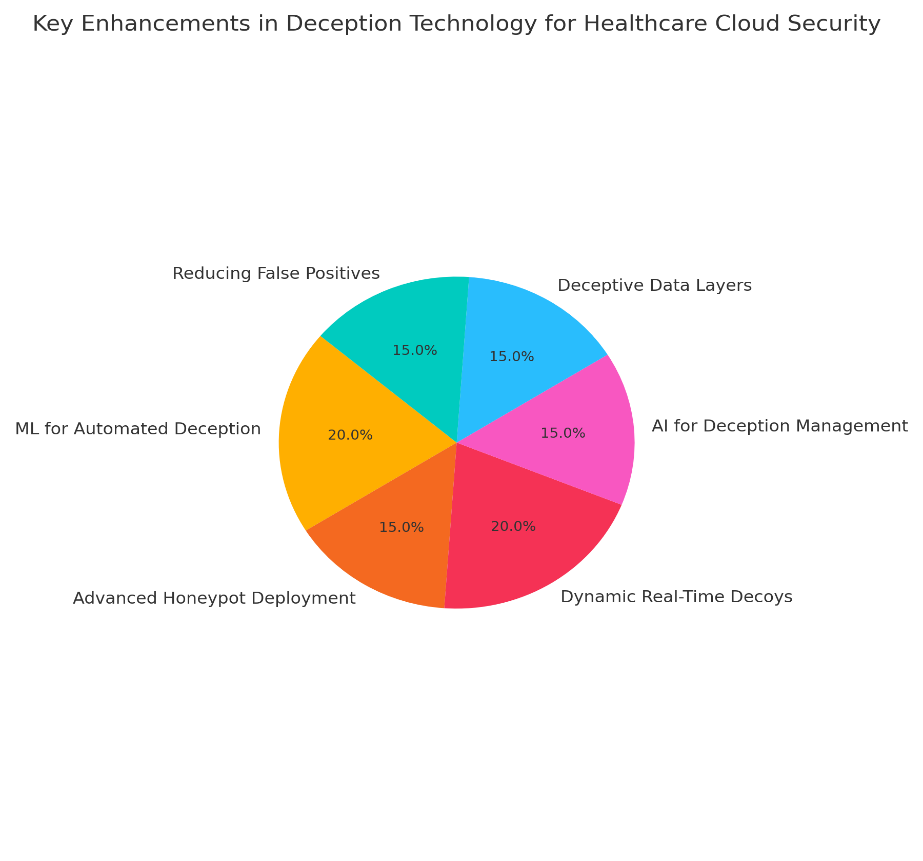
Deception technology serves as a protective shield for cloud-based health systems, luring in attackers while gathering intelligence on their activities, thereby employing active defense tactics. It plays an important role in defending sensitive patient information from sophisticated cyber threats.

The application of machine learning (ML) to automate deception is perhaps one of the most thrilling advances. With ML, self-adjusting snares, or honeypots, can be created which can evolve with the attack patterns [16], [17]. More sophisticated honeypots replicate actual healthcare infrastructure, luring attackers into elaborately staged worlds, where their actions can be monitored and analyzed by security personnel [18]

Dynamic decoy deployment employs events trigger to increase the difficulty of an attacker's attempts. An AI is capable of self-adapting and crafting realistic decoys, thus heightened deception management [19]. Deceiving patient records, which act as data buffers, moreover, protects the actual information and warns defenders of intrusions. [18], [20]In addition, security staff can concentrate their attention on real threats because alerts will only be issued when decoys are accessed [21]. Alarms that are less frequent also constitute a major advantage. The relative importance of these fundamental deception enhancements in cloud security to healthcare is shown graphically in Figure 3, which illustrates their theoretical distribution and importance.

The implementation of AI-powered decoy systems to block unauthorized access and maintain HIPAA compliance showcased the application of deception technologies in safeguarding healthcare data [22] Furthermore, the application of containerized honeypots enhanced the detection of real-time attacks and threat mitigation in cloud-based healthcare systems. These technologies enhance the security of sensitive information while simultaneously mitigating the risk of cyber threats by enticing attackers into controlled environments where they can be observed [22].

As seen in Figure 3, the reinforced cloud security deception frameworks and their relevance to healthcare have been visually represented showing their theoretical distribution and significance.



**FIGURE 3.** Key enhancement in deception technology for healthcare cloud security

## Techniques used in Deception Technology

Cloud healthcare security is becoming more empowered with Deception technology through the application of Artificial Intelligence (AI) and Machine Learning (ML). Technology are applied to create realistic decoys automatically that simulate components like electronic health records, diagnostic machines, and Internet of Things (IoT) medical devices. Through the application of models like transformers and neural networks, the system learns in real-time to simulate attackers' behavior, which makes the decoys more lifelike. This not only increases the effectiveness of deception but also facilitates proactive threat detection and continuous development of defensive capabilities [23]

Healthcare infrastructures also employ a variety of decoy-based methods such as honeypots, breadcrumbs, and emulated medical resources to mislead attackers. High-interaction honeypots are designed to resemble real healthcare services such as remote access or imaging devices to attract attackers. Breadcrumbs such as emulated credentials or configuration files are strategically deployed to attract attackers into a trap. The methods help security professionals to capture valuable information about attacker methods while maintaining real systems at minimal risk [24]

Deception is also enhanced by integration with Security Orchestration, Automation, and Response (SOAR) platforms. This enables healthcare systems to respond instantly when attackers interact with decoys—triggering alerts, analyzing activity using SIEM tools, and automatically responding such as isolating threats or triggering countermeasures. In highly regulated healthcare environments, such instant responses reduce exposure, aid compliance, and enable forensic investigation [25]

## Challenges in Deception Technology Techniques.

Cloud health systems use decoy realistic assets, which will attract attackers to bypass actual sensitive data. Decoys are things like simulation login details, SSH tokens, and ghost servers simulating actual patient databases or hospital services. As soon as the attacker has reached the decoy asset, the system monitors the contact and notifies security teams. The breach is detected early, and lateral movement through the network is evaded [26]

Deception systems place fake artifacts (e.g., credentials, cookies, or files) into real systems that mislead attackers to decoys. The artifacts raise an alarm and enable behavior analysis on contact. The technique is extremely effective in the healthcare industry, where one needs to detect illegal access to patient histories early without compromising real data [27]

Healthcare cloud environments today possess sophisticated deception systems incorporating artificial intelligence and machine learning. Such systems provide real-time simulation of adaptive deception scenarios, with improved scalability and realism for decoys. Some examples are mobile honeypots and dynamically evolving decoy networks for threat information collection and disorienting long-lasting attackers, slowing them down significantly [28]

## Mitigate the Challenges in Implementing Deception Technology

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly being applied to deception technology in order to automate the generation of realistic decoys, such as fake medical reports or activity of IoT devices [29][30]. The AI systems learn in real time to adapt to threat activities, improving anomaly detection and reducing false positives, with high availability [31]

Incorporating SOAR and SIEM with deception technology may lead to concerns such as alert exhaustion and an overabundance of notifications. These issues can be resolved with the implementation of AI and ML models which can effectively prioritize notifications according to the pattern of the attack. An example of this would be a reinforcement learning model that dynamically changes the behavior of the decoys so that only important threats activate responses and deceptions do not trigger responses unnecessarily [32].

Deception would be most effective when integrated with tools such as SOAR and SIEM to enable real-time threat identification and automated response to threats. For example, interactions with decoys like simulated RDP or PACS servers might trigger automatic containment responses, enhancing visibility into security and response times—while being HIPAA and GDPR compliant.

As healthcare data is sensitive, the strategies of deception must be in accordance with legal and ethical demands. This encompasses anonymizing decoy data and keeping these separate from real patient data, and having the deception specifically focus on targeting criminal malicious actors. Employing audit logs and monitoring devices ensures compliance and responsibility in accordance with the legal framework.

# CONCLUSIONS

To wrap up, deception technology presents a forward-looking, impactful method for bolstering cloud security in the healthcare sector by deploying decoy environments and intelligent traps that identify and misdirect intruders. This approach sharpens threat visibility, lowers the rate of false alarms, and aligns with regulatory frameworks such as HIPAA and GDPR. While alert exhaustion and ethical dilemmas pose hurdles, ongoing improvements in artificial intelligence and seamless fusion with SOAR and SIEM platforms position deception as a meaningful complement to established defenses, enabling healthcare organizations to safeguard sensitive patient information more effectively amid the continuously shifting digital environment.

# REFERENCES

1. T. Alsuwaidani, “The security challenges in healthcare cloud computing,” Int. J. Comput. Sci. Netw. Secur. **22**(3), 731 (2022).
2. F. Javadpour, T. Ja’fari, T. Taleb, M. Shojafar, and C. Benzaïd, “A comprehensive survey on cyber deception techniques to improve honeypot performance,” Comput. Secur. **140**, 103792 (2024).
3. R. W. Anwar, T. Abdullah, and F. Pastore, “Firewall best practices for securing smart healthcare environment: A review,” Appl. Sci. **11**(19), 9183 (2021).
4. P. K. Chouhan and G. S. Aujla, “Deception technology for active defence: Background and opportunities,” Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops), 1183–1188 (2024).
5. P. S. Samant, “Secure cloud services for the healthcare industry: Addressing unique challenges and ensuring compliance,” Int. J. Res. Appl. Sci. Eng. Technol. **12**(4), 3095–3101 (2024).
6. H. Arif, F. Hoda, and A. Kumar, “Establishing cloud security by setting up honeypot on Azure services,” (2023).
7. Z. Morić, V. Dakić, and D. Regvart, “Advancing cybersecurity with honeypots and deception strategies,” Informatics **12**(1), 14 (2025).
8. D. Morais, F. G. Pinto, I. M. Pires, N. M. Garcia, and A. J. Gouveia, “The influence of cloud computing on the healthcare industry: A review of applications, opportunities, and challenges for the CIO,” Procedia Comput. Sci. **204**, 714–720 (2022).
9. M. Mehrtak et al., “Security challenges and solutions using healthcare cloud computing,” J. Med. Life **14**(6), 769–774 (2021).
10. S. Kumar and D. K. Shaw, “Efficient access requests management for healthcare data with security and privacy-preserving,” Expert Syst. Appl. **257**, 126194 (2025).
11. “Examination of mindfulness-based self-efficacy of students studying in sports sciences,” J. Educators Teachers Trainers **13**(5), 541–549 (2022).
12. R. Sivan and Z. A. Zukarnain, “Security and privacy in cloud-based e-health system,” Symmetry **13**(5), 742 (2021).
13. J. Pateria, L. Ahuja, and S. Som, “Critical path to place decoys in deception biota,” Int. J. Performability Eng. **18**(12), 854–862 (2022).
14. F. Süß, M. Freimuth, A. Aßmuth, G. R. S. Weir, and B. Duncan, “Cloud security and security challenges revisited,” arXiv:2405.11350 (2024).
15. F. Al-Tawara and A. Khalifeh, “Recent challenges, issues, and initiatives for cloud computing adoption in healthcare: A survey,” Proc. Int. Conf. Control, Decision Inf. Technol. (CoDIT), 409–415 (2023).
16. Z. Aradi and A. Bánáti, “The role of honeypots in modern cybersecurity strategies,” Proc. IEEE World Symp. Appl. Mach. Intell. Informat. (SAMI), 189–196 (2025).
17. P. Shojaei, E. Vlahu-Gjorgievska, and Y. W. Chow, “Security and privacy of technologies in health information systems: A systematic literature review,” Computers **13**(2), 41 (2024).
18. S. Ahmed, A. B. M. M. Rahman, M. M. Alam, and M. S. I. Sajid, “SPADE: Enhancing adaptive cyber deception strategies with generative AI and structured prompt engineering,” Proc. IEEE Annu. Comput. Commun. Workshop Conf. (CCWC), 1302–1307 (2025).
19. L. Zhang and V. L. L. Thing, “Three decades of deception techniques in active cyber defense—Retrospect and outlook,” Comput. Secur. **105**, 102288 (2021).
20. R. Jain and N. Nihalani, “Recent developments in botnet detection tools and techniques for IoT security: A review,” Proc. Int. Conf. Advancements Key Challenges Green Energy Comput. (AKGEC), (2024).
21. Z. Morić, V. Dakić, and D. Regvart, “Advancing cybersecurity with honeypots and deception strategies,” Informatics **12**(1), 14 (2025).
22. V. S. D. Priya and S. S. Chakkaravarthy, “Containerized cloud-based honeypot deception for tracking attackers,” Sci. Rep. **13**, 28613 (2023).
23. J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, “A survey of honeypots and honeynets for Internet of Things, Industrial Internet of Things, and cyber-physical systems,” IEEE Commun. Surv. Tutor. **23**(4), 2351–2383 (2021).
24. G. Sreedevi, T. N. Harshitha, V. Sugumaran, and P. Shankar, “Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review,” Inf. Process. Manag. **59**(2), 102888 (2022).
25. O. U. Oluoha, T. S. Yange, G. E. Okereke, and F. S. Bakpo, “Cutting edge trends in deception-based intrusion detection systems—A survey,” J. Inf. Secur. **12**(4), 250–269 (2021).
26. J. Zou, Z. Sun, C. Ku, X. Li, and A. Dahbura, “WiP: Developing high-interaction honeypots to capture and analyze region-specific bot behaviors,” (2024).
27. M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, “Machine learning for Healthcare-IoT security: A review and risk mitigation,” IEEE Access **11**, 145869–145896 (2023).
28. D. Liebowitz et al., “Deception for cyber defence: Challenges and opportunities,” Proc. IEEE Int. Conf. Trust, Privacy, Security Intell. Syst. Appl. (TPS-ISA), 173–182 (2021).
29. P. Osinuga, J.-J. Chin, and T. S. C. Lau, “Implementing identity-based signature schemes for secure data transfer in cloud computing environments,” Journal of Informatics and Web Engineering. 4(1), 111–128 (2025). https://doi.org/10.33093/jiwe.2025.4.1.9.
30. A. Hashmi, N. Amjad, M. M. Ullah Satti, U. Hayat, and A. Mumtaz, “Exploring big data management approaches and applications: A case study of real-time data analytics in air traffic management,” *J. Informatics Web Eng.* **4**(2), 339–352 (2025). https://doi.org/10.33093/jiwe.2025.4.2.21
31. O. Akinade, P. A. Adepoju, A. B. Ige, and A. I. Afolabi, “Cloud security challenges and solutions: A review of current best practices,” Int. J. Multidiscip. Res. Growth Eval. **6**(1), 26–35 (2024).
32. A. Alabdulatif and N. N. Thilakarathne, “A novel cloud-enabled cyber threat hunting platform for evaluating the cyber risks associated with smart health ecosystems,” Appl. Sci. **14**(20), 9567 (2024).