ISSN: 2755-6190

Research Article

Open Access Journal of Artificial Intelligence and Technology

Cloud Computing and Cybersecurity in Human-Centric Intelligent Systems

Chery Ann Alexander[1] and Lidong Wang[2*]

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

[*]Corresponding author
Lidong Wang, Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA.

Received: December 18, 2025; **Accepted:** December 29, 2025; **Published:** January 05, 2026

ABSTRACT
Cloud computing provides a scalable, flexible, and accessible infrastructure for human-centric intelligent systems (HCIS). Cybersecurity plays a crucial role in enabling HCIS and maintaining the functions of HCIS. This paper presents cloud computing and cybersecurity in general areas/fields and highlights cloud computing and cybersecurity in the HCIS of healthcare, which includes multidisciplinary topics and applications research. This research includes a cyber risk management framework; a cloud shared responsibility model, an attack model, and the life cycle of identity and access management; a security shared responsibility model and security across a pipeline; the theories and principles of cloud computing and cybersecurity in general areas/fields (major theories and principles, improvements in the theories and principles, and the testing of the improvements); and the theories and principles of cloud computing and cybersecurity in the HCIS of healthcare (major theories and principles, improvements, and the testing of the improvements in the HCIS of healthcare). The evaluation and improvement of tools, data, and processes of the cloud and cybersecurity in a medical center (Charleston Regional Medical Center in the US) are presented as a case study.

Keywords: Human-Centric Intelligent Systems (HCIS), Artificial Intelligence (AI), Cloud Computing, Cybersecurity, Healthcare, Privacy Preservation, User Behaviors

Introduction

Human-centric intelligent systems (HCIS) are based on artificial intelligence (AI), considering human needs, values, and experiences. Cloud computing provides a scalable, flexible, and accessible infrastructure for HCIS. Cybersecurity plays a key role in enabling HCIS and maintaining the functions of HCIS. Robust cybersecurity helps amplify and enhance HCIS. A human-centric intelligent cybersecurity recognizes human vulnerabilities (such as susceptibility to social engineering and using weak passwords), deals with human behaviors related to cybersecurity, and reduces human errors and insider threats. Cloud compliance and legal challenges were identified as major concerns for consumers. 49% of consumers were concerned with cloud integration with the organization's IT environment, and 62% were concerned with data leakage [1]. Cloud compliance is always a concern for an organization, as responsibilities and accountabilities become driven by contracts. A cloud security comparator system was developed for customers who plan to move their data to the cloud but are uncertain due to security concerns. There are several standards being developed for cloud data by organizations like the National Institute of Standards and Technology (NIST), International Organization for Standards (ISO), and Cloud Security Alliance [2].

Cyber incident effects can be: 1) unauthorized use-an attacker utilizes system resources for illegitimate purposes, 2) interruption-making an information asset of a system become unavailable or unusable, 3) interception-gaining unauthorized access to asset or information, 4) fabrication-inserting false information or components into a system, 5) modification causing a change in the protocol, data, software, or hardware of an IT resource, and 6) degradation causing a decrease in the performance of an IT resource [3].

There have been standards and frameworks that offer a strategic approach to cloud computing security, including International Standard Organization (ISO) 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework

Citation: Chery Ann Alexander, Lidong Wang. Cloud Computing and Cybersecurity in Human-Centric Intelligent Systems. Open Access J Artif Intel Tech. 2026. 2(1): 1-10. DOI: doi.org/10.61440/OAJAIT.2026.v2.17

(CSF), Cloud Security Alliance (CSA), and the Federal Risk and Authorization Management Program (FedRAMP). ISO 27001 begins with establishing context by identifying internal and external issues. The first NIST CSF function is identified with asset management for a category. CSA offers a control specification to conduct an independent audit and assurance evaluation. FedRAMP is based on the NIST 800-53 security control catalog and Federal Information Processing Standards (FIPS) 199 standard for security categorization. Performing a risk evaluation for cloud computing platforms is a challenge in the space of Information Security Management Systems. ISO 27001 risk evaluation techniques have been employed for Alcohol Monitoring Systems. Scaling localized methods to international and national cloud security standards is not an issue of 'one size fits all'. The methods and context for performing cloud risk evaluation were investigated across representative international and national standards and guidelines [4].

To sufficiently introduce the information security management system (ISMS) and the security management framework (SMF) into a cloud computing environment, principles and recommendations of the ISMS standards should be modified and included in the cloud computing management system, and the traditional SMF should be improved by proactive and predictive security controls, proactive forensic infrastructure, and mandatory digital forensic investigation process. The ISO has developed the ISO 27001 and ISO 27002 standards. The challenges of implementing ISO 27001 standard controls in a cloud environment were discussed. ISO 27002 covers the following 11 domains [5].

- Information security policy
- Organization of information security
- Human resource security
- Access controls
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- Information security incident management
- Information security aspects of business
- Continuity management
- Compliance

Migration of organizational data to the cloud is a strategic but complicated decision. Security challenges should be mitigated before the data is moved into the cloud. Various security measures (e.g., firewalls and intrusion detection systems) and the types of encryption and authentication techniques should be checked. The state of eHealth security issues in the cloud was analyzed, including regulatory (such as HIPAA) issues. Both HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) ask users (within the healthcare provider's organization) to be held accountable for their behaviors when treating patients' protected health information (PHI) [6]. The primary purpose of the research in this paper is to deal with cloud computing and cybersecurity in HCIS. The remainder of this paper will be organized as follows: the second section introduces a cyber risk management framework; the third section presents a cloud shared responsibility model, an attack model, and the life cycle of identity and access management; the fourth section presents a security shared responsibility model and security across a pipeline; the fifth section introduces the theories and principles of cloud computing and cybersecurity in general areas/fields; the sixth section presents the theories and principles of cloud computing and cybersecurity in the HCIS of healthcare; the seventh section presents case study regarding the evaluation and improvement of the tools, data, and processes of the cloud and cybersecurity in a medical center; and the eighth section is conclusion and future research.

A Cyber Risk Management Framework

A cyber risk management framework was developed in which risk management activities are organized and assessed in four layers, as illustrated in Figure 1. All four layers are intricately intertwined and closely referenced to the cyber risk management framework, enabling comprehensive cyber risk management to be realized. The cyber ecosystem layer is regarding identifying and understanding the roles of stakeholders. The cyber infrastructure layer is responsible for safeguarding an organization's IT assets and services. The cyber risk assessment layer focuses on the identification of cyber risks, risk quantification, and cyber investment analysis. The cyber performance layer is regarding the actual development and operation of a cybersecurity system based on performance goals set at the risk assessment layer [7].

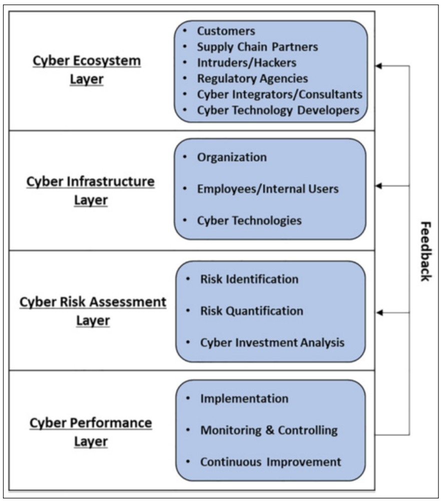

Figure 1: A cyber risk management framework [7].

A Cloud Shared Responsibility Model, an Attack Model, and the Life Cycle of Identity and Access Management

A cloud shared responsibility model is illustrated in Figure 2. Determining how to grant access to data in services or applications is nearly always the customer's responsibility in a cloud environment. When employing SaaS, the application security is the provider's responsibility, but there may be security-relevant configuration items that are the customer's responsibility. The middleware security can be the customer's responsibility (for IaaS), the provider's responsibility (for PaaS), or the shared responsibility (for SaaS). In an Infrastructure-as-a-Service environment, the virtualized infrastructure (virtual network, virtual machines, storage) is the cloud provider's responsibility [8].

The Cyber Security Game (CSG) has been used to quantitatively identify cybersecurity risks. A risk score is computed by utilizing a mission impact model to calculate the consequences of cyber incidents. Figure 3 illustrates an attack model and how the topology affects an attacker, assuming that the first try and attack is on the client host Win 7–2. S is defined as a successful compromise, and OIC refers to attackers Outside trying to get in by attacking a client situation. Win 7–2 can also become compromised by a malicious insider with Inside Access (IA). Host Win 7–1 is the Same Type of Client (STC) as Win 7–2. The Linux host is a client computer of a Different Type of Client (DTC) than Win 7–1. All the P(*|*) in the figure represents the probability [3].

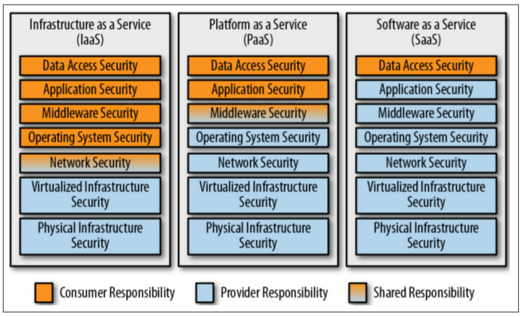
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Data Access Security
Application Security
Middleware Security
Operating System Security
Network Security
Virtualized Infrastructure Security
Physical Infrastructure Security
Consumer Responsibility
Provider Responsibility
Shared Responsibility

Figure 2: A cloud shared responsibility model [8].

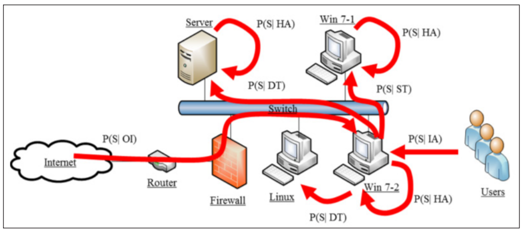

Figure 3: An attack model [3].

Identity and access management (IAM) is possibly the most significant set of security controls. Figure 4 illustrates both creation and deletion of identities along with the creation and deletion of access rules for these identities. Identity and access can be managed by the same system or different systems [8].

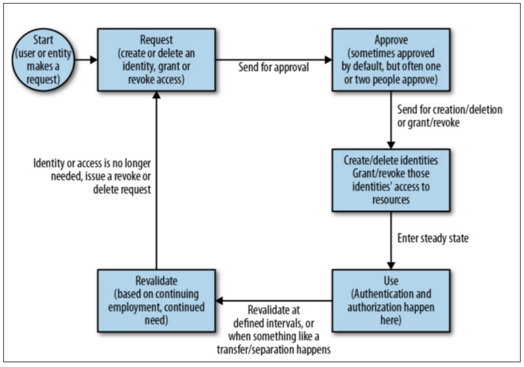
Start (user or entity makes a request)
Request (create or delete an identity, grant or revoke access)
Send for approval
Approve (sometimes approved by default, but often one or two people approve)
Send for creation/deletion or grant/revoke
Create/delete identities Grant/revoke those identities' access to resources
Enter steady state
Use (Authentication and authorization happen here)
Revalidate at defined intervals, or when something like a transfer/separation happens
Revalidate (based on continuing employment, continued need)
Identity or access is no longer needed, issue a revoke or delete request

Figure 4: A life cycle of identity and access management (IAM) [8].

A Security Shared Responsibility Model and Security across a Pipeline

The basics of cloud computing, cloud migration strategy, cloud computing security models, concerns about public cloud security, and how to address them by using practical approaches were studied. The security challenges and problems of private cloud computing models were examined. Possible practical approaches to overcoming the challenges and minimizing security risks were analyzed. Cloud security has no defined perimeter due to multiple cloud actors involved in making things happen in the environment. Regardless of public or private cloud deployment models, cloud security should be an integral part of an overall cloud adoption project [9]. Figure 5 illustrates what Amazon Web Services (AWS) is responsible for and what a cloud consumer is responsible for to build and run the infrastructure-as-a-service (IaaS) layer. AWS offers its cloud security responsibility model, which is illustrated in Figure 6. A security reference architecture was proposed to secure the application build, testing, deployment, and running tasks. In a modern agile-based software development model, the plan, code, build, test, release, and deployment processes are part of the process of development and operations (DevOps) in the software development lifecycle (SDLC). Integrating security in the process of DevOPS makes it DevSecOps (short for development, security, and operations), which highlights that security should be at each step of the process or pipeline, as illustrated in Figure 7 [9].

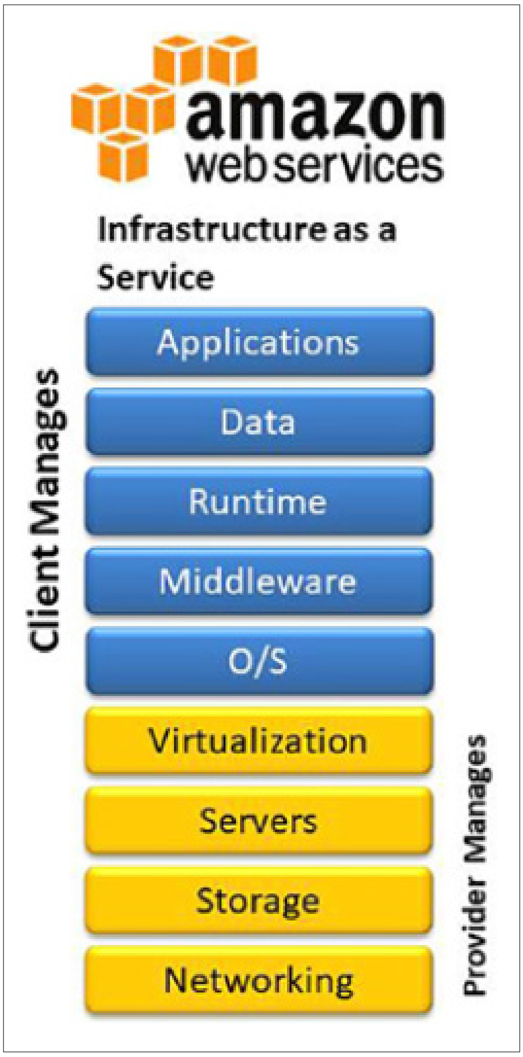

Figure 5: Amazon Web Services – IaaS: consumer responsibility vs. provider responsibility [10].

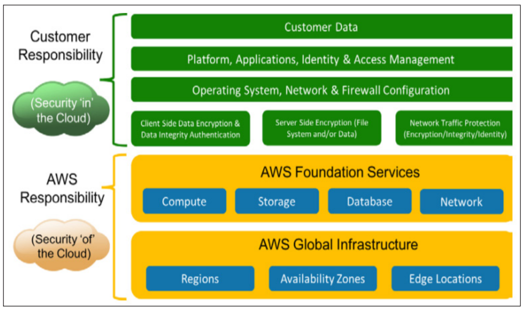
Customer Responsibility
(Security 'in' the Cloud)
Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client Side Data Encryption & Data Integrity Authentication
Server Side Encryption (File System and/or Data)
Network Traffic Protection (Encryption/Integrity/Identity)
AWS Responsibility
(Security 'of' the Cloud)
AWS Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations

Figure 6: Amazon Web Services – IaaS: security shared responsibility model [10].

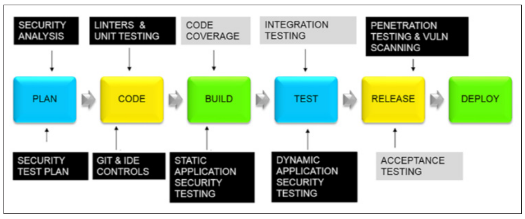

Figure 7: DevSecOps: security across the pipeline [11].

Theories and Principles of Cloud Computing and Cybersecurity in General Areas/Fields

Major Theories and Principles of Cloud Computing and Cybersecurity

Cloud computing and cybersecurity are interconnected. Cloud computing offers infrastructure (focusing on on-demand access to computing resources over the Internet) while cybersecurity offers the security framework and practices to guarantee that cloud environments are secure and resilient against cyberthreats. Cloud computing is of technology, while cybersecurity is the security applied to technology. Theories of cloud computing and cybersecurity encompass concepts, frameworks, and models that guide the design and execution of secure cloud environments. These theories deal with both technical and organizational aspects of security, focusing on confidentiality, integrity, and availability (CIA) of cloud resources [12]. Major theories or principles of cloud computing and cybersecurity in general areas are listed in Table 1.

Table 1: Major Theories and Principles of Cloud Computing and Cybersecurity in General Areas/Fields [12].

Theories	Details
Institutional Theory	Examining how external pressures (e.g., regulations & industry standards) affect the adoption of cloud security & practices.
Deterrence Theory	Discouraging potential attackers by making the cloud environment more difficult & costly to breach (e.g., by performing multi-factor authentication, strong encryption, & regular security audits).
Diffusion of Innovation	Focusing on how new technologies are implemented by organizations & individuals over time.
Shared Responsibility Model	Cloud providers & cloud users share responsibility for security in cloud environments (with providers securing the infrastructure & users securing their data as well as applications).
Technology Acceptance Model	Exploring how user perceptions of ease of use & perceived usefulness influence the acceptance or adoption of cloud computing.
Three pillars of security (fundamental principles)	Confidentiality, integrity, availability (CIA).
Compliance & governance	Following regulatory requirements (e.g., HIPAA & GDPR).
Technology Organization Environment	Examining the impact of technological, organizational, & environmental factors on the adoption of cloud computing.
Cloud security frameworks	• Cloud Security Frameworks: Frameworks such as the NIST Cybersecurity Framework (CSF) & the Cloud Security Alliance's Cloud Controls Matrix (CCM) help to build a holistic cloud security strategy. • NIST CSF delivers a structured approach to managing cybersecurity risks, with functions of Identify, Protect, Detect, Respond, & Recover. • Cloud Security Alliance's CCM offers a holistic set of security controls for cloud environments, supporting compliance & risk management.
Other theories	• Game theory (analyzing interactions between a defender & an attacker). • Social learning theory (understanding how an individual learns & adopts security behaviors). • Situational crime prevention theory (changing the environment to decrease opportunities for crime).

Improvements in the Theories and Principles of Cloud Computing and Cybersecurity

Cloud computing security is continuously evolving, with improvements focusing on zero-trust architectures, cloud-native security tools, the automation of security processes, etc. Improving cloud security theories and practices needs to embrace innovative technologies such as AI/ML, while also dealing with existing challenges such as compliance, visibility, and the skills gap. Continuous learning, adaptability, and collaboration are significant [13]. Major improvements in the theories, principles, and practices of cloud computing and cybersecurity, and challenges and future directions in general areas are listed in Table 2.

Table 2: Major Improvements in the Theories, Principles, And Practices of Cloud Computing and Cybersecurity, And Challenges and Future Directions in General Areas/Fields [14].

Aspects	Details
Cybersecurity Mesh Architecture (CSMA)	Modular security approaches such as CSMA are crucial in hybrid & multi-cloud environments, enabling centralized oversight & decentralized control over security.
Security automation & orchestration	• Employing AI/ML to automate threat detection, incident response, & policy enforcement, improving efficiency & reducing human error in a dynamic cloud environment. • DevSecOps integrates security into the software development lifecycle, automating security checks & vulnerability evaluations.
Unified security management	Unified security management: Unified platforms provide centralized visibility & control across heterogeneous cloud environments, simplifying security management & dealing with the complexities of multi-cloud deployments.
Zero Trust Architecture	These principal highlights "never trust, always verify", continuously verifying user devices, identities, & access privileges.
Dealing with evolving threats	Cloud security needs continuous evaluation & adaptation to combat sophisticated threats, involving utilizing AI/ML & cloud-native security tools for real-time threat detection & response.
Challenges & future directions	• AI-enabled security challenges: Challenges (such as data privacy, interpretability, & adversarial attacks) due to AI should be addressed while AI provides noteworthy benefits. • Lack of visibility: Inadequate visibility into a cloud environment leads to a challenge in detecting misconfigurations, compliance violations, & unauthorized access. • Managing a rapidly evolving attack surface: The dynamic nature of the cloud expands the attack surface, necessitating continuous monitoring & vulnerability scanning. • Complicated regulatory compliance: Navigating complicated data protection & privacy regulations in the cloud needs continuous tracking of updates, understanding legal requirements, & aligning the security strategy. • Integration with emerging technologies: The combination of AI with quantum computing (QC) & other emerging technologies provides new opportunities for cloud security.

Testing of Improvements in the Theories and Principles of Cloud Computing and Cybersecurity

Testing improvement in cloud computing security theories involves a systematic approach that integrates theoretical assessment with practical applications and ongoing monitoring. Based on a systematic approach, security controls can be measured, and improvements in cloud computing security theories can be effectively tested and validated [14]. Table 3 illustrates how the advancements in cloud computing and cybersecurity theories in general areas can be tested.

Table 3: Testing of Improvements in the Theories, Principles, and Practices of Cloud Computing and Cybersecurity in General Areas/Fields [14].

Aspects	Details
Defining the theory & expected improvements	Clearly articulate the specific cloud computing security theory & the intended improvements planned to test.
Establishing clear metrics	Establishing relevant cloud security metrics to track improvement. Examples include a reduced number of security incidents, faster incident response times, and lower security costs.
Choosing a testing approach	Common approaches are Black Box (no prior knowledge), Gray Box (limited information), & White Box (deep knowledge of infrastructure) testing.
Selecting suitable testing techniques	Testing techniques can be: • Penetration testing (simulating real-world attacks to identify exploitable vulnerabilities & weaknesses in the cloud environment). • Vulnerability evaluation (employing automatic tools to scan for known vulnerabilities & misconfigurations in the cloud infrastructure & applications). • Application Programming Interface (API) security testing. • Automating & integrating testing (integrating automation tools for continuous security testing. • Threat modeling (creating threat models to understand potential attack scenarios & align testing efforts with specific risks). • Code review (manually examining the source code of cloud applications to identify potential coding vulnerabilities).

Selecting suitable testing techniques	• Automated security validation (using tools that automate security testing & monitor cloud security continuously). • Security audits (performing regular security audits to evaluate encryption, access controls, network security, & compliance with related regulations). • Automatic security validation: Utilizing tools that automate security testing & monitor cloud security continuously.
Monitoring & analyzing results	• Continuously monitoring the cloud environment employing real-time threat detection systems, automatic security tools, & security information and event management (SIEM) systems. • Analyzing the collected data & logs to identify patterns, weaknesses, & the influence of the implemented theory on cybersecurity.
Assessment & refinement	• Evaluating results: Analyzing the test results to decide if the improvements have improved security & mitigated identified risks. • Refining the theory/implementation: Based on the results, refining the security theory or its implementation to deal with any identified gaps or weaknesses.
Documenting & reporting findings	• Detailing the testing process, findings, and the influence of the implemented theory on cloud security. • Communicating results & recommendations to related stakeholders.
Continuous improvement	Performing post-testing reviews & continuously updating the testing approach with new technologies & best practices.

Theories and Principles of Cloud Computing and Cybersecurity in the HCIS of Healthcare

Major Theories and Principles of Cloud Computing and Cybersecurity in the HCIS of Healthcare

Cloud security in healthcare involves protecting sensitive patient data while leveraging the benefits of cloud computing. Theories of cloud computing and cybersecurity in healthcare involve strategies, frameworks, and methods that a healthcare organization utilizes to protect systems and patient data in cloud environments [15]. Major theories or principles of cloud computing and cybersecurity in healthcare are listed in Table 4.

Table 4: Major Theories or Principles of Cloud Computing and Cybersecurity in Healthcare [16].

Theories	Details
Shared Responsibility Model	• A cloud provider & a healthcare organization share responsibility for cloud security. The specific division of responsibility depends on the cloud service model (IaaS, PaaS, SaaS) & the cloud provider. • A provider is responsible for the underlying infrastructure's security, while a healthcare organization is responsible for data & application security in the cloud.
Threat modeling	Identifying & mitigating potential security risks & vulnerabilities by modeling & analyzing a system and data flow.
Layered security approach	A holistic cloud security strategy includes multiple layers of security controls: data encryption, access control & identity management, continuous monitoring & threat detection, regular security audits & compliance checks, backup & disaster recovery, & employee training.
Principle of least privilege	Giving a user the minimum necessary access rights to finish his/her job reduces the potential security breaches.
Regulatory compliance	Complying with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) & the General Data Protection Regulation (GDPR) for patient data privacy & security.
Cloud security frameworks	• NIST CSF offers a structured approach to managing cybersecurity risks & can be employed together with healthcare regulations such as HIPAA. • ISO 27001 (an international standard) provides a framework to manage cloud security risks through holistic risk evaluations & control execution.
Diffusion of Innovation	Utilizing blockchain technology for data integrity, AI/ML for threat detection, & zero trust security models to enhance security in healthcare.

Improvements in the Theories and Principles of Cloud Computing and Cybersecurity in the HCIS of Healthcare

A healthcare organization can improve cloud security greatly by utilizing technological advancements and an improved awareness of the importance of protecting patient data while keeping compliance with regulations [16]. Major improvements in the theories, principles, and practices of cloud computing and cybersecurity in healthcare are listed in Table 5.

Table 5: Major Improvements in the Theories, Principles, and Practices of Cloud Computing and Cybersecurity in Healthcare [16].

Aspects	Details
Leveraging advanced theories & technologies	• Zero-Trust Security Models: No entity is trusted by default, requiring verification for all access requests. • AI/ML: Proactively analyzing user behaviors to flag suspicious activities, detecting threats, & automating responses. • Hybrid cloud strategy: The hybrid cloud model, combining public & private clouds, permits a healthcare organization to use public clouds for less sensitive tasks while using the security of private clouds for sensitive data.
Improved threat detection & response	• AI-powered threat detection: Integrating AI/ML into cloud security tools to analyze large datasets in real-time, identify abnormal patterns, & detect threats fast. • Behavioral analysis: Analyzing user behaviors using AI/ML & flagging unusual activities that might indicate a security breach. • Automated abnormal detection: Improved anomaly detection based on AI/ML, providing proactive alerts for prompt investigation & mitigation of potential threats.
Dealing with emerging technologies in healthcare	• Telemedicine and remote care: Robust cloud security is important for protecting sensitive patient data transmitted during virtual consultations & remote patient monitoring. • Cloud-based health analytics: Secure & scalable cloud solutions are significant for analyzing large datasets to improve patient outcomes while sustaining security. • Integration of IoT and medical devices: Strong security measures are required to protect the data collected by IoT or IoMT devices due to potential vulnerabilities or risks in these devices.
Enhanced data security measures	• Blockchain technology: Creating tamper-proof digital records, guaranteeing data integrity & traceability (especially beneficial for healthcare data sharing & storage), improving interoperability & patients' control over their data. • End-to-end encryption: Data encryption for data in transit or at rest guarantees data is unreadable to unauthorized parties.

Testing of Improvements in the Theories and Principles of Cloud Computing and Cybersecurity in the HCIS of Healthcare

A systematic approach that integrates technical evaluations with ongoing monitoring and assessment is required to test improvements in cloud computing security theories in healthcare, protect sensitive patient data, and comply with regulations such as HIPAA. To test the improvements on cloud computing security theories in healthcare, it is necessary to create a baseline, rigorously test their effectiveness using various techniques, measure and analyze the results, and create a process for continuous monitoring and improvement [17]. Table 6 shows how the improvements in the theories of cloud computing and cybersecurity in healthcare could be tested.

Table 6: Testing Improvements in the Theories, Principles, and Practices of Cloud Computing and Cybersecurity in Healthcare [17].

Aspects	Details
Defining clear objectives, scope, & metrics	• Specifying the security goal & specific security theories or practices. • Defining the scope of the testing (which cloud assets, applications, and data will be assessed?). • Defining main metrics to track progress towards the security goal. These could include incident response time, vulnerability reduction rate, compliance adherence, etc.
Performing various testing methods	• Penetration testing: Simulating real-world attacks to evaluate the resilience of the cloud environment against potential breaches. • Vulnerability scanning: Employing automatic tools to systematically scan for known vulnerabilities & misconfigurations in the cloud environment. • Risk evaluations: Regularly identifying potential threats & vulnerabilities, prioritizing remediation based on impact & likelihood. • Security auditing: Regularly auditing cloud services, data flow, access controls, & security configurations to guarantee that they align with policies & identify weaknesses. • Regular compliance checks: Guaranteeing compliance with regulatory requirements (such as HIPAA) by performing regular compliance checks. • Security code reviews: Reviewing application code to identify potential security issues.

Analyzing & documenting results	• Keeping comprehensive logs: Keeping detailed logs of all security assessments, audits, & incident response activities. • Analyzing results & identifying trends. • Reporting findings & recommendations: Providing clear and concise reports on the results of security evaluations & audits, including recommendations for remediation.
Continuous improvement	• Post-testing reviews: Conducting reviews after testing to identify lessons learned and areas for improvement. • Adapt strategies: Continuously updating the cloud security testing strategy to incorporate new technologies, threat trends, & industry best practices.

A Case Study

The Evaluation of the Tools, Data, and Processes of the Cloud and Cybersecurity in a Medical Center

Charleston Regional Medical Center in the US is a hospital that serves patients from a radius of central to western areas of Mississippi. At any given time, the patient census may be 900-4,000 patients, with approximately 1,000 inpatients. The medical center makes significant use of public cloud systems. It is also facing noteworthy cybersecurity threats and vulnerabilities in medical devices, cloud systems, etc., resulting in data breaches, disruptions in patient care, and considerable financial losses. The assessment of cloud tools, data, and processes and cybersecurity in the Medical Center involves evaluating their suitability for handling sensitive patient information, guaranteeing secure and reliable data management, and optimizing performance. Main considerations lie in security, compliance, interoperability, scalability, and cost-effectiveness. By selecting the right cloud platform, executing strong security controls, and streamlining workflows, the Medical Center can use the cloud to revolutionize patient care and deliver excellent services. Table 7 shows the tools, data, and processes of the cloud in the Medical Center [18].

Table 7: The Tools, Data, And Processes of the Cloud in the Medical Center

Aspects	Details
Tools	• Cloud platforms: Major cloud providers provide healthcare services (e.g., secure data storage). The Medical Center evaluates which platform best suits its specific needs & guarantees compliance with regulations such as HIPAA. • Specialized healthcare cloud tools: Many tools are available for data migration, AI/ML & data analytics, security & compliance, disaster recovery, etc. • Electronic health record (EHR) systems: Cloud-based EHR systems provide enhanced accessibility, interoperability, & scalability. • Telehealth & remote monitoring: Cloud technology helps telemedicine & remote patient monitoring, improving access to care & enabling continuous data capture from medical devices.
Data	• Data variety: A cloud platform needs to process various data formats (structured, semi-structured, & unstructured) from different sources (e.g., patient records, medical images, & clinical notes). • Data velocity: Cloud services enable rapid scaling of computing resources to process data in real-time for applications (e.g., patient monitoring). • Data integrity: Cloud solutions guarantee data integrity (preventing modifications or corruption). • Data security & privacy: Healthcare data, such as protected health information (PHI), requires strict security measures. Cloud services adhere to HIPAA compliance, following data encryption, access controls, audit trails, & breach notification procedures.
Processes	Data migration & integration, data analytics based on AI/ML, information sharing, collaboration & communication, workflow optimization & automation, remote patient monitoring, risk management, disaster recovery & business continuity, etc.

The Improvement of the Tools, Data, and Processes of the Cloud and Cybersecurity in the Medical Center

The improvement of cloud tools, data, and processes and cybersecurity in the Medical Center involves a number of crucial strategies to deal with challenges and leverage the benefits of cloud adoption. By focusing on these, the Medical Center can effectively leverage cloud technology to strengthen data management, improve operational efficiency, and eventually deliver better patient care. Table 8 shows how to improve cloud tools, data, and processes in the Medical Center [19].

Table 8: Improving The Tools, Data, And Processes of the Cloud in the Medical Center

Aspects	Details
Tools	• Advanced analytics based on AI/ML: Employing cloud-based tools for advanced data analytics (based on AI/ML) to improve the functions of tools, increase diagnosis accuracy, and enhance operational efficiency & cybersecurity. • Secure collaboration platforms: Cloud-based platforms provide HIPAA-compliant messaging & secure data sharing for improved communication & collaboration among healthcare professionals.
Data	• Centralized data repositories: Utilizing cloud services to create centralized data repositories that consolidate patient data from various sources, making it more accessible & easier to analyze. • Real-time data collection & analysis: Integrating cloud services with Internet of Medical Things (IoMT) devices & wearables for real-time data capture & analysis.
Processes	• Cloud migration strategy: Developing a strategy for migrating healthcare data & applications to the cloud. • Optimization & scalability: Continuously monitoring & optimizing cloud resource utilization to decrease costs & guarantee scalability.

Conclusion and Future Research

Theories of cloud computing and cybersecurity encompass concepts, frameworks, and models that guide the design and execution of secure cloud environments. Cloud computing security is continuously evolving, with improvements focusing on zero-trust architectures, cloud-native security tools, the automation of security processes, etc. Improving cloud security theories and practices needs to embrace innovative technologies such as AI/ML, while also dealing with existing challenges such as compliance, visibility, and the skills gap. Testing improvement in cloud computing security theories involves a systematic approach that integrates theoretical assessment with practical applications and ongoing monitoring. Theories of cloud computing and cybersecurity in the HCIS of healthcare involve strategies, frameworks, and methods that a healthcare organization utilizes to protect systems and patient data in cloud environments. A healthcare organization can improve cloud security greatly by utilizing technological advancements and an improved awareness of the importance of protecting patient data while keeping compliance with regulations.

A systematic approach that integrates technical evaluations with ongoing monitoring and assessment is required to test improvements in cloud computing security theories in healthcare. It is necessary to create a baseline, rigorously test the effectiveness using various techniques, measure and analyze the results, and create a process for continuous monitoring and improvement. Assessing cloud tools, data, and healthcare processes involves evaluating their suitability for handling sensitive patient information, guaranteeing secure and reliable data management, and optimizing performance. Main considerations lie in security, compliance, interoperability, scalability, and cost-effectiveness. By selecting the right cloud platform, executing strong security controls, and streamlining workflows, a healthcare organization can use the cloud to revolutionize patient care and deliver excellent services. Improving cloud tools, data, and processes in healthcare involves a number of crucial strategies to deal with challenges and leverage the benefits of cloud adoption. By focusing on these, a healthcare organization can effectively leverage cloud technology to strengthen data management, improve operational efficiency, and eventually deliver better patient care. The same AI capabilities that improve cybersecurity can be weaponized by malicious actors. Defenses against AI malicious actors for cloud-based HCIS and the ethical use of AI within cloud-based HCIS are our future research.

Acknowledgements

The authors would like to express they're thanks to Technology and Healthcare Solutions, USA, for its help and support.

Author Contributions

Ideation: CAA. Conceptualization, investigation, and methodology: CAA, LW. Writing original draft preparation: CAA. Review and editing: LW

Availability of data and materials: Not applicable

Declarations

Conflict of interest Authors declare that there is no conflict of interest

References

1. Cloud Security Alliance (CSA). Cloud Security Alliance Study Identifies New and Unique Security Challenges in Native Cloud, Hybrid and Multi-Cloud Environments. Plus, Company Updates. 2019.
2. Joshi KP, Elluri L, Nagar A. An Integrated Knowledge Graph to Automate Cloud Data Compliance. IEEE Access, Access, IEEE. 2020. 8: 148541-148555.
3. Musman S, Turner A. A game theoretic approach to cyber security risk management. The Journal of Defense Modeling and Simulation. 2018. 15: 127–146.
4. Weil TR. Standards for Cloud Risk Assessments-What's Missing? 2020 IEEE Cloud Summit. 2020. 11–17.
5. Arafat M. Information security management system challenges within a cloud computing environment. Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018. 1-6.
6. Al-Issa Y, Ottom MA, Tamrawi A. Health Cloud security challenges: A survey. Journal of Healthcare Engineering. 2019. 2019: 7516035.
7. Lee I. Cybersecurity: Risk management framework and investment cost analysis. Business Horizons. 2021. 64: 659-671.

8. Dodson C. Practical Cloud Security: a guide for secure design and deployment. O'Reilly Media, Inc., USA. 2019.
9. Jeganathan S. Practical approaches to overcome security challenges in cloud computing. ISSA Journal. 2018. 16: 30-41.
10. Scott S. AWS Shared Responsibility Model: Cloud Security, Cloud Academy. 2017.
11. Porter T. DevSecOps - A New Chance for Security. DZone. 2018.
12. Amini M, Jahanbakhsh Javid N. A multi-perspective framework established on diffusion of innovation (DOI) theory and technology, organization and environment (TOE) framework toward supply chain management system based on cloud computing technology for small and medium enterprises. Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises (January 2023). International Journal of Information Technology and Innovation Adoption. 2023. 11: 1217-1234.
13. Kakkad V, Shah H, Patel R, Doshi N. A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing. Procedia Computer Science. 2019. 155: 680-685.
14. Marinescu DC. Cloud computing: theory and practice. Morgan Kaufmann. 2022.
15. Conteh FJ. A Holistic Insight into the Privacy and Security of Cloud-Based Computing Approach on Healthcare Information Management Systems in the United States–A Grounded Theory Approach, Doctoral Dissertation, Marymount University, Arlington, Virginia, USA. 2024.
16. Akinsanya OO. Maturity Model for Healthcare Cloud Security. Ph.D. Dissertation, University of Plymouth, UK. 2020.
17. Tilahun N. The Application of Quantitative Methods in the Adoption of Cloud Computing Within a Framework of Unified Technology Acceptance Theory: a Comparative Analysis of US Hospitals Ntitled Item, Doctoral dissertation, Purdue University, West Lafayette, Indiana, USA. 2023.
18. Senthilkumar SA, Rai BK, Meshram AA, Gunasekaran A, Chandrakumar Mangalam S. Big data in healthcare management: a review of literature. American Journal of Theoretical and Applied Business. 2018. 4: 57-69.
19. Devarajan MV. Improving security control in cloud computing for healthcare environments. J. Sci. Technol. JST. 2020. 5.

Copyright: © 2026 Lidong Wang, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.