https://doi.org/10.48047/AFJBS.6.12.2024.4969-4978

AFJBS African Journal of Biological Sciences
Journal homepage: http://www.afjbs.com

Research Paper   Open Access

Navigating the Security and Privacy Landscape in Cloud Computing: Challenges, Solutions, and Future Directions

Atluri Sunada Priya [1], Nallamilli Revathi Reddy [2], Jonnalagadda Thrishitha [3], Ramaiah Challa [4], Likhita Samayamanthula [5], S.S. Aravinth [6]

[1] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. sunadapriya@gmail.com*

[2] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. revathireddyn1@gmail.com*

[3] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. thrishitha11@gmail.com*

[4] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. ramaiah.challa@kluniversity.in*

[5] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. likhita2278@gmail.com*

[6] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur. aravinthkrithick@gmail.com*

Article History
Volume 6, Issue 12, 2024
Received: June 10, 2024
Accepted: July 5, 2024
doi:
10.48047/AFJBS.6.12.2024.4969-4978

Abstract-Cloud computing has developed as a disruptive tool for businesses, providing scalability, flexibility, and cost effectiveness. However, outsourcing data and applications to third-party cloud providers raises serious concerns about security and privacy. This literature study digs into the diverse terrain of security and privacy challenges that arise in cloud systems, concentrating on characteristics such as confidentiality, integrity, availability, accountability, and privacy preservation. It investigates many security frameworks and approaches offered in the literature, such as encryption, access control, intrusion detection systems, and trustworthy cloud computing frameworks. Furthermore, the analysis covers security flaws unique to mobile cloud computing. Future research directions and recommendations for reducing security vulnerabilities in cloud computing are also addressed. Overall, the evaluation underlines the need of thoroughly addressing security and privacy concerns to ensure The ongoing success and deployment of cloud computing technology.

Keywords: Component, Formatting, Style, Styling, Insert.

1. Introduction

Cloud computing has emerged as a transformative force in the realm of Information Technology (IT), reshaping the landscape of how businesses of all sizes access and utilize computing resources. Offering unparalleled scalability, flexibility, and cost-effectiveness, cloud-based data storage solutions have become increasingly prevalent in today's digital era.

However, amidst the myriad benefits that cloud computing offers, there exists a pressing concern regarding the security and privacy of data entrusted to third-party cloud providers. This comprehensive literature review seeks to explore the multifaceted landscape of security and privacy issues inherent in cloud environments, with a specific focus on five key attributes: confidentiality, integrity, availability, accountability, and privacy-preservability. As organizations transition towards cloud-based infrastructures, they encounter both opportunities and challenges. While cloud environments facilitate optimal resource utilization and easy access to computing resources over the Internet, they also introduce security vulnerabilities, particularly due to the migration of assets outside administrative control in a shared environment. Addressing these security concerns necessitates a multifaceted approach, as evidenced by recent literature proposing various frameworks and techniques aimed at protecting data throughout its lifecycle in cloud environments. These solutions encompass a wide array of measures, including encryption techniques, access control mechanisms, intrusion detection systems (IDS), and trusted cloud computing frameworks. Additionally, the review extends its discussion to explore security vulnerabilities specific to mobile cloud computing (MCC), shedding light on challenges such as data leakage, insecure communication channels, and device theft. cloud computing continues to evolve rapidly, it becomes imperative to address open issues and chart future research directions in cloud security. This includes the exploration of novel security concepts and recommendations, the development of advanced intrusion detection and prevention frameworks, and the establishment of robust security compliance mechanisms. while cloud computing holds immense potential to revolutionize the IT landscape, it is crucial to comprehensively address security and privacy concerns to ensure the integrity and confidentiality of data entrusted to cloud environments. Through a meticulous literature review and exploration of proposed solutions and future research directions, organizations can gain a deeper understanding of cloud security issues and devise proactive strategies to mitigate risks effectively.

2. Literature Review

Cloud computing has emerged as a revolutionary paradigm in the realm of Information Technology (IT), offering unparalleled scalability, flexibility, and cost-effectiveness to businesses of all sizes. However, alongside its numerous benefits, the outsourcing of data and applications to third- party cloud providers has brought forth substantial concerns regarding security and privacy. This comprehensive literature review aims to delve into the multifaceted landscape of security and privacy issues inherent in cloud environments, with a keen focus on five key attributes: confidentiality, integrity, availability, accountability, and privacy-preservability. The shared and elastic nature of cloud environments presents both opportunities and challenges. While it enables optimal utilization of hardware resources and facilitates easy access to computing resources over the Internet, it also introduces security vulnerabilities, particularly due to the migration of assets outside administrative control in a shared environment. Addressing these security concerns requires a multifaceted approach. Recent literature proposes various frameworks and techniques aimed at protecting data throughout its lifecycle in cloud environments. These solutions encompass encryption techniques, access control mechanisms, intrusion detection systems (IDS), and trusted cloud computing frameworks. Furthermore, the discussion extends to security vulnerabilities specific to mobile cloud computing (MCC), highlighting challenges such as data leakage, insecure communication channels, and device theft. As cloud computing continues to evolve, it becomes imperative to address the open issues and future research directions in cloud security. This includes the exploration of new security concepts and recommendations, the development of advanced intrusion detection and prevention frameworks, and the establishment of robust security compliance mechanisms. while cloud computing offers unparalleled potential to revolutionize the IT landscape, it is essential to address security and privacy concerns comprehensively. By conducting a thorough literature review and exploring proposed solutions and future research directions, organizations can enhance their understanding of cloud security issues and develop proactive strategies to mitigate risks effectively. Cloud computing has emerged as a pivotal technology in meeting the ever-growing demands of modern organizations. With its promise of simplified IT infrastructure, remote accessibility, and cost efficiencies, cloud-based data storage solutions have garnered significant attention. the adoption of cloud computing is accompanied by inherent security and privacy challenges that necessitate further exploration. researchers from academia, industry, and standards organizations have provided potential solutions to address the security and privacy challenges in cloud computing. The narrative review presented in this survey delves into the various components of cloud computing and elucidates the security and privacy problems these systems face. The review identifies key security issues and requirements in cloud computing, including confidentiality, integrity, availability, and privacy preservation. Moreover, it highlights known threats and vulnerabilities that pose risks to cloud environments. By analyzing different components of cloud computing, the review aims to provide a holistic understanding of the security challenges faced by cloud entities, including cloud service providers, data owners, and cloud users.

3. Cloud Security Issues and Challenges

Cloud security issues and challenges in cloud computing have become increasingly prominent as organizations continue to adopt cloud-based data storage solutions. While cloud computing offers unparalleled scalability, flexibility, and cost-effectiveness, the outsourcing of data and applications to third-party cloud providers introduces significant concerns regarding security and privacy. One of the primary challenges in cloud security is ensuring confidentiality, integrity, and availability of data stored in the cloud. The shared and elastic nature of cloud environments presents opportunities for optimal resource utilization but also introduces vulnerabilities, particularly due to the migration of assets outside administrative control in a shared environment. This poses risks of unauthorized access, data breaches, and service disruptions, compromising the security and integrity of sensitive information. Addressing these security concerns requires a multifaceted approach that encompasses various frameworks and techniques aimed at protecting data throughout its lifecycle in cloud environments. Encryption techniques, access control mechanisms, intrusion detection systems (IDS), and trusted cloud computing frameworks are among the solutions proposed in recent literature to mitigate security risks in cloud computing. However, challenges persist in implementing and managing these security measures effectively across diverse cloud environments. The emergence of mobile cloud computing (MCC) introduces additional security vulnerabilities, including data leakage, insecure communication channels, and device theft. As organizations increasingly rely on mobile devices to access cloud services, ensuring the security of data transmitted and stored on these devices becomes paramount. Future research directions in cloud security include the exploration of new security concepts and recommendations, the development of advanced intrusion detection and prevention frameworks, and the establishment of robust security compliance mechanisms. Collaboration between academia, industry, and standards organizations is essential to address evolving threats and vulnerabilities effectively and to enhance the overall security posture of cloud environments. While cloud computing offers numerous benefits to organizations, it is essential to prioritize cloud security to mitigate risks effectively. By identifying and addressing security issues and challenges comprehensively, organizations can enhance their understanding of cloud security and develop proactive strategies to safeguard sensitive information in cloud environments.

4. Cloud Computing Security

Cloud computing security is a critical aspect of the paradigm's adoption and utilization, given its transformative potential in the realm of Information Technology (IT). While cloud computing offers unparalleled scalability, flexibility, and cost-effectiveness to businesses, the outsourcing of data and applications to third-party cloud providers raises substantial concerns regarding security and privacy. The multifaceted landscape of cloud environments presents both opportunities and challenges in terms of security. The shared and elastic nature of cloud infrastructures enables optimal utilization of hardware resources and facilitates easy access to computing resources over the Internet. However, this shared environment also introduces security vulnerabilities, particularly due to the migration of assets outside administrative control. Addressing these security concerns necessitates a multifaceted approach. Recent literature proposes various frameworks and techniques aimed at protecting data throughout its lifecycle in cloud environments. These solutions encompass encryption techniques, access control mechanisms, intrusion detection systems (IDS), and trusted cloud computing frameworks.

The above figure 1 illustrates that effective cloud security integrates governance, compliance, IAM, availability, and security. Proper planning and controls are essential for a secure and compliant cloud environment.

5. Security Policies in Cloud Computing

Cloud computing has revolutionized the IT landscape, offering unparalleled scalability, flexibility, and cost-effectiveness to businesses. However, alongside its benefits, the outsourcing of data and applications to third-party cloud providers has raised substantial concerns regarding security and privacy. Organizations must implement robust security policies tailored to the unique challenges of cloud environments. These security policies should encompass the following key areas:

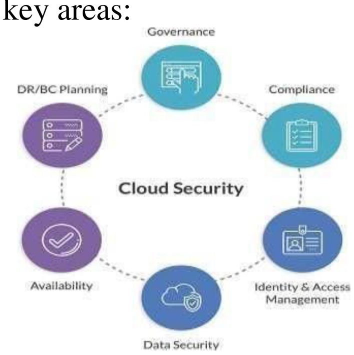

Figure 1. Cloud Security is Critical Aspect of the Para Diagram

A. Confidentiality

- **Encryption:** Implement robust encryption mechanisms to protect sensitive data from unauthorized access during storage, transmission, and processing in the cloud.
- **Access Control:** Enforce strict access control policies to ensure that only authorized users and applications can access sensitive data and resources in the cloud environment

B. Integrity

- **Data Validation:** Implement data validation mechanisms to ensure the integrity of data stored and processed in the cloud, preventing unauthorized modifications or tampering.
- **Integrity Checks:** Perform regular integrity checks and audits to detect and mitigate any unauthorized changes to data or system configurations in the cloud.

C. Availability

- **Redundancy:** Implement redundancy and failover mechanisms to ensure high availability of cloud services and resources, minimizing downtime and service disruptions.

- **Disaster Recovery:** Develop comprehensive disaster recovery plans to recover data and restore services in the event of system failures or catastrophic events.

D. Accountability

- **Logging and Monitoring:** Implement robust logging and monitoring mechanisms to track user activities, system events, and security incidents in the cloud environment.
- **Audit Trails**: Maintain detailed audit trails of user actions and system events to facilitate forensic analysis and accountability for security incidents.

E. Privacy Preservability

- **Data Minimization:** Minimize the collection and storage of personally identifiable information (PII) to reduce privacy risks and comply with data protection regulations.

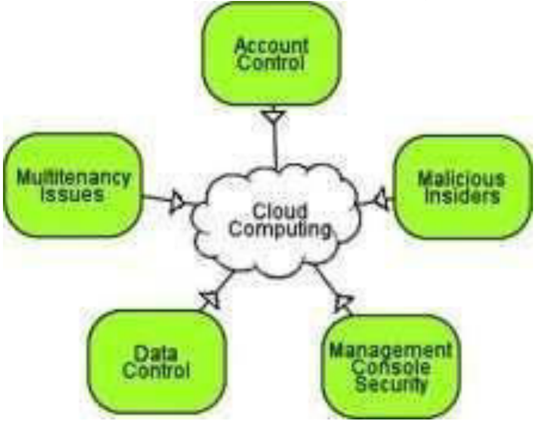

Figure 2. Cloud Computing has Revolutionized the IT Landscape

Anonymization: Implement anonymization techniques to protect the privacy of user data while still enabling meaningful analysis and processing in the cloud.

From the above figure 2, Cloud Computing has revolutionized the IT landscape but brings challenges like account control, multitenancy issues, data control, management console security, and malicious insiders.

6. Service-Level Agreement

Service-level agreements (SLAs) play a crucial role in addressing security and privacy concerns in cloud computing environments. These agreements serve as contractual agreements between cloud service providers and their customers, outlining the terms and conditions of the services being provided, including security measures and performance guarantees. In the context of security and privacy, SLAs define the responsibilities of both parties regarding the protection of sensitive data and the prevention of unauthorized access. This includes specifying encryption protocols, access control mechanisms, and data handling procedures to ensure the confidentiality, integrity, and availability of data stored in the cloud. SLAs may include provisions for compliance with industry regulations and standards, such as GDPR, HIPAA, or PCI DSS, to ensure that cloud services adhere to legal and regulatory requirements related to data privacy and security.

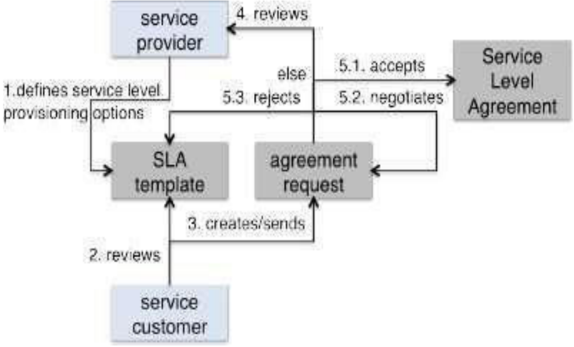

Figure 3. Service Level Arrangements

From the above figure 3, service Provider defines service level provisioning actions and reviews SLA. Service Level Agreement is created/sent, and customer negotiates and accepts.

A. Creation of Security Domains

Introducing federations, in association with PKI and LDAP technology, will lead to efficient trust relationships between involved entities. A federation refers to a group of legal entities that share a set of agreed policies and rules for accessing online resources. This structure provides a legal framework that facilitates authentication and authorization across different organizations. Cloud infrastructures can be organized into distinctive security domains, which are defined as applications or collections of applications that trust a common security token for authentication, authorization, or session management. By leveraging federations, these security domains can collaborate to form Federated Clouds comprise a collection of single clouds that can interoperate with one another. This interoperability allows for seamless data exchange and resource sharing between different cloud providers and organizations. Federated Clouds enable enhanced scalability, flexibility, and resource utilization while maintaining robust security measures. Integrating PKI (Public Key Infrastructure) and LDAP (Lightweight Directory Access Protocol) technologies into federated cloud environments, organizations can establish secure authentication and authorization mechanisms. PKI facilitates secure communication and data exchange through the use of digital certificates, while LDAP enables centralized management of user identities and access controls.

From the below Figure 4, the security domain in cloud computing protects data using cybersecurity, physical security, network security, and risk management.

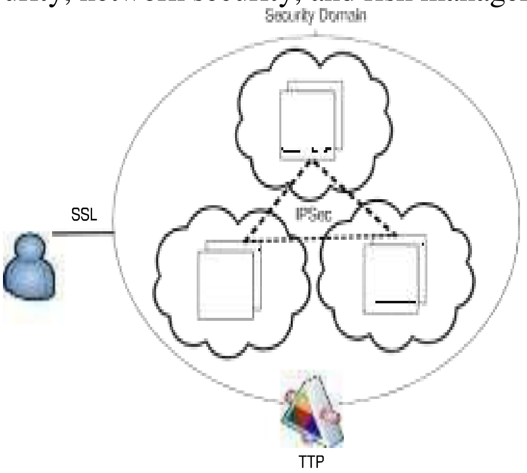

Figure 4. Security Domain

7. Framework and Techniques

To address the security and privacy challenges inherent in cloud computing, researchers have proposed a variety of frameworks and techniques aimed at enhancing data protection and mitigating security risks. These solutions encompass a multifaceted approach, incorporating encryption techniques, access control mechanisms, intrusion detection systems (IDS), and trusted cloud computing frameworks.

- **Encryption Techniques:** Encryption plays a crucial role in safeguarding data confidentiality in cloud environments. Advanced encryption algorithms, such as AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman), are utilized to encrypt data both at rest and in transit. Additionally, homomorphic encryption enables computation on encrypted data without decrypting it, preserving data privacy while allowing for secure processing in the cloud.
- **Access Control Mechanisms:** Access control mechanisms are essential for enforcing granular permissions and preventing unauthorized access to cloud resources. Role-based access control (RBAC) and attribute-based access control (ABAC) are

commonly employed to define and manage user privileges based on roles, attributes, and policies. Fine-grained access control policies enable organizations to restrict access to sensitive data and enforce least privilege principles.

- **Intrusion Detection Systems (IDS):** Intrusion detection systems are deployed to detect and respond to security incidents and anomalies in cloud environments. Host-based IDS monitor system activities on individual cloud instances, while network-based IDS analyze network traffic for signs of malicious activity. Additionally, anomaly detection techniques, such as machine learning algorithms, are utilized to identify deviations from normal behavior and alert administrators to potential security threats.
- **Trusted Cloud Computing Frameworks:** Trusted cloud computing frameworks aim to establish trust and transparency in cloud services by implementing standardized security controls, certifications, and audits. Industry standards, such as ISO/IEC 27001 for information security management and SOC 2 (Service Organization Control) for data privacy and security, provide guidelines for cloud service providers to demonstrate compliance with security best practices and regulatory requirements.
- **Emerging Technologies:** Advancements in emerging technologies, such as blockchain and secure multi-party computation (SMPC), offer innovative solutions to enhance cloud security and privacy. Blockchain technology provides a decentralized and immutable ledger for recording transactions and verifying data integrity, while SMPC enables collaborative computation on encrypted data without revealing sensitive information to any party.

8. Discussions

The conversation around cloud computing security and privacy issues emphasizes how important it is to take a comprehensive approach to solving the various problems that businesses confront. Although cloud computing provides unmatched scalability, flexibility, and affordability, there are serious concerns about confidentiality, integrity, availability, accountability, and privacy preservation when data and applications are outsourced to outside providers. A variety of frameworks and strategies, such as encryption, intrusion detection systems, access control mechanisms, and trusted cloud computing frameworks, have been proposed in recent literature to address these security challenges. To remain ahead of new threats and weaknesses, cloud computing is dynamic and requires constant study and innovation. The conversation also touches on security issues unique to mobile cloud computing, highlighting the necessity for solutions to deal with device security, unsecured communication channels, and data leakage. Organizations need to make resolving unresolved issues and investigating potential avenues for cloud security research their top priorities going ahead. This entails creating strong security compliance procedures, investigating novel security ideas and recommendations, and creating sophisticated intrusion detection.

Table 1. Cloud Computing Security and Privacy Issues Emphasizes

Cyber-security system features		**Privacy Implications and suggested analysis**
Dimension	**Type**	
Architecture of system	Standalone (hardware protection system), Client-server or Collaborative (host-based security suites)	[Exp] Check whether sensor data are communicated in plain text or not. Communicate sensor data to the gateway through a secure channel (elliptic curve cryptography). Communicate data from the home gateway to remote entities using an encrypted channel.

Type of Detection	Anomaly-based or Signature-based (depending on the used HIDS and HIPS products)	[Id] [Sens] [Freq] Home sensor data, especially if observed on the long term, may reveal sensitive information (presence, routines, medical conditions) or reveal the user's identity. Check specific data and degree of re-identifiability/sensitivity.
Ecosystem	Mobile Devices, IoT	[Sens] High data sensitivity (activities, habits, personal data). Check for sensitive data. Check for risks of inferring additional sensitive data. [Ctrl] Limited user control.
Type of Data	Application, Network	[Sens] Some kinds of sensor data are inherently sensitive (audio-video streams), other kinds may be used to infer sensitive data (number of inhabitants, personal lifestyle. [Id] The user's identity may be reconstructed based on the home gateway IP address or Web activity. Check degree of re-identifiability.

9. Result

The thorough literature study that cloud computing benefits organizations greatly, providing them with cost-effectiveness, scalability, and flexibility. These advantages do, however, come with serious security and privacy risks. Confidentiality, integrity, availability, accountability, and privacy-preservability are the five main characteristics of security and privacy challenges in cloud systems that are highlighted in the review. Cloud settings present a range of opportunities and problems due to their shared and elastic nature. Although it makes it easier to access computing resources and maximizes resource utilization, the fact that assets in a shared environment are not under administrative control creates security concerns. To address these security problems, a number of frameworks and methods have been put forth, such as intrusion detection systems (IDS), encryption, access control mechanisms, and trustworthy cloud computing frameworks. Furthermore, particular issues with mobile cloud computing (MCC) are brought to light, including insecure communication pathways and data leakage. The review emphasizes how crucial it is to address un resolved problems and potential avenues for future research in cloud security, such as investigating novel security ideas, creating sophisticated frameworks for intrusion detection and prevention, and putting in place reliable security compliance systems. In conclusion, even though cloud computing has enormous potential to completely transform IT environments, security and privacy issues must be thoroughly addressed. Through detailed literature studies, investigation of suggested solutions, and exploration of future research possibilities, organizations can improve their understanding of these issues and create proactive plans to effectively manage risks.

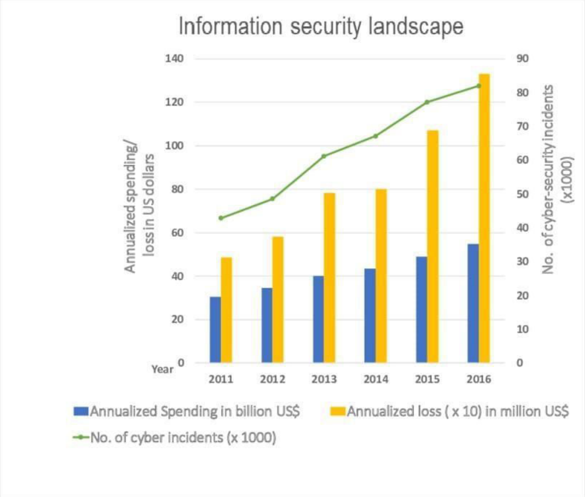

Figure 5. Security Landscape

From the Above Figure 5, The data was regarding the United States' yearly expenditure on cybersecurity The US Office of Management and Budget provides the data on cyber-security events that have been reported in the United States.

10.Conclusion

In summary, the development of cloud computing has brought about a new era in information technology (IT) that is characterized by scalability, flexibility, and cost-effectiveness. But in addition to all of its advantages, outsourcing data and apps to outside cloud providers has brought to light serious privacy and security issues. The various security and privacy concerns present in cloud environments have been clarified by this thorough literature analysis, which highlights important characteristics including confidentiality, integrity, availability, accountability, and privacy-preservability. It has brought attention to how cloud environments are elastic and shared, which presents both potential and security vulnerability challenges. Recent literature suggests that addressing these security challenges calls for a multidimensional strategy that combines a variety of frameworks and strategies aimed at securing data throughout its lifecycle in cloud-based settings. Additionally, the review has looked into security flaws unique to mobile cloud computing (MCC), highlighting issues including device theft and data leaks. It is critical to address outstanding challenges and future research paths in cloud security as cloud computing continues to develop. This involves investigating novel ideas in security, creating sophisticated frameworks for detecting and preventing intrusions, and putting strong security compliance systems in place. Ultimately, even while cloud computing has the unmatched potential to completely transform the IT industry, security and privacy issues must be thoroughly addressed. Organizations may fully utilize cloud computing while protecting sensitive data and maintaining the integrity of cloud environments by improving our awareness of cloud security challenges and creating proactive measures to successfully minimize risks.

References

[1] Z. Xiao and Y. Xiao, “Security and Privacy in Cloud Computing,” IEEE Communications Surveys & amp; Tutorials, vol. 15, no. 2, pp. 843–859, 2013. doi:10.1109/surv.2012.060912.00182.

[2] H. Takabi, J. B. D. Joshi, and G.-J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments,” IEEE Security &amp; Privacy Magazine, vol. 8, no. 6, pp. 24–31, Nov. 2010.
doi: 10.1109/msp.2010.186.

[3] S. K. Sood, “A combined approach to ensure data security in cloud computing,” Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, Nov. 2012.
doi: 10.1016/j.jnca.2012.07.007.

[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.
doi: 10.1109/tpds.2010.183.

[5] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” The Journal of Supercomputing, vol. 76, no. 12, pp. 9493–9532, Feb. 2020.
doi: 10.1007/s11227-020-03213-1.

[6] S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” Journal of Network and Computer Applications, vol. 75, pp. 200–222, Nov. 2016.
doi: 10.1016/j.jnca.2016.09.002.

[7] M. A. Khan, “A survey of security issues for cloud computing,” Journal of Network and Computer Applications, vol. 71, pp. 11–29, Aug. 2016, doi: 10.1016/j.jnca.2016.05.010.

[8] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, “Security Issues for Cloud Computing,” International Journal of Information Security and Privacy, vol. 4, no. 2, pp. 36–48, Apr. 2010.
doi: 10.4018/jisp.2010040103.

[9] A. Nagarajan and V. Varadharajan, “Dynamic trust enhanced security model for trusted platform based services,” Future Generation Computer Systems, vol. 27, no. 5, pp. 564–573, May 2011.
doi: 10.1016/j.future.2010.10.008.

[10] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing,” IEEE Access, vol. 7, pp. 74361–74382, 2019.
doi: 10.1109/access.2019.2919982.

[11] Ranaweera, P., Jurcut, A. D., & Liyanage, M. (2021). Survey on Multi-Access Edge Computing Security and Privacy. IEEE Communications Surveys &amp; Tutorials, 23(2), 1078–1124. https://doi.org/10.1109/comst.2021.3062546

[12] S. El Kafhali, I. El Mir, and M. Hanini, “Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing,” Archives of Computational Methods in Engineering, vol. 29, no. 1, pp. 223–246, Apr. 2021, doi: 10.1007/s11831-021- 09573-y.

[13] X. Yang et al., “A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges,” IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 2, pp. 273–302, Feb. 2021.
doi: 10.1109/jas.2020.1003536.

[14] K. Zhang, X. Song, C. Zhang, and S. Yu, “Challenges and future directions of secure federated learning: a survey,” Frontiers of Computer Science, vol. 16, no. 5, Dec. 2021.
doi: 10.1007/s11704- 021-0598-z.

[15] J. L. Hernandez-Ramos et al., “Security and Privacy in Internet of Things-Enabled Smart Cities: Challenges and Future Directions,” IEEE Security &amp; Privacy, vol. 19, no. 1, pp. 12–23, Jan. 2021.
doi: 10.1109/msec.2020.3012353