Educational Administration: Theory and Practice
2024, 30(6), 1193 - 1198
ISSN: 2148-2403
https://kuey.net/

Research Article

Application Layer Security For Cloud

Ripalkumar Patel[1*], Amit Goswami[2], Hirenkumar Kamleshbhai Mistry[3], Chirag Mavani[4]

[1*]Software Developer, Emonics, Email: Ripalpatel1451@gmail.com
[2]Software Developer, Source Infotech, Email: amitbspp123@gmail.com
[3]Sr. System Administrator, Zenosys LLC, Email: hiren_mistry1978@yahoo.com
[4]Devops Engineer, DXC Technology, Email: chiragmavanii@gmail.com

Citation: Ripal Kumar Patel, et.al (2024) Application Layer Security For Cloud, *Educational Administration: Theory And Practice, 30(6), 1193 - 1198*
Doi: 10.53555/kuey.v30i6.5468

ARTICLE INFO

ABSTRACT

The rapid emergence and evolution of cloud computing have revolutionized the way organizations and individuals manage their data. However, this new technology also comes with its own set of security issues. The paper investigates the security concerns that arise when it comes to using cloud computing. It will help researchers and practitioners identify the most effective ways to protect their organizations from these threats. The paper explores the critical role that the application layer plays in the delivery of cloud services. It highlights the numerous vulnerabilities in this component that allow it to be exploited for various attacks, such as distributed denial of service and SQL injection. It also emphasizes the importance of following regulatory standards, such as HIPAA and GDPR, in order to protect sensitive information. This paper explores the various security techniques that can be used to protect an organization's cloud computing applications. Some of these include multi-factor authentication and encryption techniques. It also suggests the use of continuous monitoring and firewalls. The paper is based on the findings of a survey, which provides recommendations for improving the security of an organization's cloud computing applications. Through the sharing of knowledge and best practices, organizations can manage the complexity of their cloud computing environment.

Keywords: Cloud computing, application layer security, cyber threats, encryption, multi-factor authentication, secure coding practices.

INTRODUCTION:

Cloud computing[1] has revolutionized the way organizations and individuals handle data and computing resources by offering flexible, scalable, and cost-effective solutions. These capabilities enable businesses to quickly scale their operations and reduce costs by leveraging shared resources and infrastructure. However, with these benefits come significant security challenges, particularly at the application layer[2].

The network model's application layer is responsible for providing users with the services that are available in the cloud. It encompasses all the applications and services that users interact with, including web applications, APIs, and various cloud-based software. Because it interfaces directly with end-users, it is frequently the primary target for cyber-attacks[3].

The application layer involves direct interaction with users, making it a visible and accessible target for attackers. Vulnerabilities at this layer can lead to immediate and severe consequences, such as data breaches, unauthorized access, and service disruption[4].

Applications handle sensitive data, including personal information, financial details, and intellectual property. Ensuring robust security measures are in place is critical to protect this data from unauthorized access and breaches[5].

Applications must manage and store user data securely to maintain user privacy. Compliance with privacy regulations (such as GDPR, HIPAA, and CCPA) is mandatory, requiring stringent data protection measures [6]. Organizations must adhere to various regulatory standards that mandate specific security practices and controls [7].

The application layer faces a wide range of security threats, including SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and distributed denial of service (DDoS) attacks. Advanced threats such as

man-in-the-middle (MitM) attacks, session hijacking, and advanced persistent threats (APTs) add to the complexity of securing this layer[8].
Implementing robust security measures at the application layer is essential. This includes encryption (both data-at-rest and data-in-transit), multi-factor authentication (MFA), secure coding practices, and the use of application firewalls (WAFs and RASP). Continuous monitoring and regular security audits are also necessary to identify and mitigate vulnerabilities promptly[9].
The cloud computing application layer is a vital part of the system, and it requires strict security measures to safeguard sensitive information. As cloud services continue to evolve and become more integral to business operations, the importance of securing the application layer will only grow. This survey paper aims to explore the current state of application layer security in the cloud, examine the existing threats and solutions, and outline best practices and future research directions.

RELATED WORKS:

Authors[10] conducted an extensive survey of the protocols that are used in the Internet of Things (IoT) application layer. They focused on the security threats that are prevalent in the industry. In this article, the authors[11] discuss the latest advances in the protocols of the Internet of Things (IoT) system and their importance in various use cases, such as healthcare and industrial IoT. They also talked about machine learning as a potential solution for the dynamic intelligence and security of the protocols.
The authors[12] of this study looked into the security of the protocols used in the Internet of Things (IoT) application layer, focusing on the CoAP protocol. They also talked about ways to address these issues, such as implementing key management systems and compressing mechanisms.
The goal of this study [13] is to explore the security implications of machine learning on the Internet of Things (IoT) application layer. The authors talk about the various techniques that can be used to enhance the layer's security.
The potential of the Internet of Things (IoT) to improve the efficiency and quality of life is discussed in this paper[14]. However, it is also emphasized that cybersecurity is very important to protect the sensitive data that is collected and stored in the network. This paper aims to provide an overview of the various security requirements of the IoT.
As organizations start to adopt cloud computing, the authors [15] of this study examine the various security threats that can affect the operations of such systems. They also talk about the best practices and countermeasures that can be used to improve the security of these systems. This paper aims to help companies make informed decisions regarding their cloud computing environment.
The authors [16] discuss the various security issues that cloud-native services face due to their distributed nature. These include the susceptibility of their infrastructure to attacks such as distributed denial of service (DDoS), malware, and man-in-the-middle (MITM). The study also provides valuable insight for cybersecurity practitioners.
The paper[17] provides a comprehensive analysis of the security challenges faced by the application layer on the Internet of Things. It explores the prevalent protocols used in the exchange of data and messages and for service discovery.
The paper [18] covered the various security concerns that apply to the protocols of the application layer. It also investigated the different types of attacks that can occur against them. The authors [19] highlight the widespread adoption of IoT across various industries and the emerging significance of edge computing, which enhances computational capacity for tasks like executing Deep Neural Networks. They note that the optimal integration of IoT, edge, and cloud computing layers remains an open research area, and review application layer protocols for connecting these layers.
This paper[20] explores the various security threats that cloud computing poses, focusing on the importance of maintaining confidentiality, integrity, privacy, and availability for both the consumers and the providers. It also highlights the role that IaaS plays in the evolution of next generation delivery models. The summary of related works is shown in table 1.

Table I. Overview of related works

Paper	Focus/Topic	Key Points
[10]	IoT Application Layer Protocols & Security Threats	- Survey of IoT protocols and prevalent security threats. - Importance of protocols in healthcare, industrial IoT. - Discussion on machine learning for protocol security.
[12]	Security of CoAP Protocol in IoT Application Layer	- Focus on CoAP protocol security. - Addressing issues with key management and compression. - Solutions for enhancing security at the application layer.
[13]	Machine Learning Implications on IoT Application Layer	- Exploration of machine learning's impact on IoT security. - Techniques for enhancing application layer security. - Consideration of dynamic intelligence and protocol security
[14]	IoT Potential & Cybersecurity	- Discussion on IoT's benefits and cybersecurity concerns. - Emphasis on protecting sensitive data in IoT networks.

		- Overview of IoT security requirements.
[15]	Cloud Computing Security Threats & Best Practices	- Examination of security threats in cloud computing. - Discussion on best practices and countermeasures. - Aim to assist companies in making informed decisions regarding cloud security.
[16]	Cybersecurity Challenges in Cloud-Native Services	- Addressing cybersecurity challenges in distributed cloud-native services. - Identification of vulnerabilities and threats. - Provision of insights for enhancing cloud-native security.
[17]	Security Challenges in IoT Application Layer	- Analysis of security challenges in IoT application layer. - Exploration of prevalent protocols and service discovery. - Insights into securing data exchange and communication in IoT.
[18]	Security Concerns & Attacks on Application Layer Protocols	- Examination of security concerns and attack types in application layer protocols. - Discussion on vulnerabilities and mitigation strategies. - Emphasis on protocol-level security measures.
[19]	Integration of IoT, Edge, and Cloud Computing Layers	- Overview of IoT adoption and emerging edge computing significance. - Review of protocols for connecting IoT, edge, and cloud layers. - Identification of open research areas in layer integration
[20]	Security Threats in Cloud Computing & Role of IaaS	- Exploration of security threats in cloud computing. - Focus on confidentiality, integrity, privacy, and availability. - Highlighting the role of IaaS in next-generation delivery models.

CURRENT STATE OF APPLICATION LAYER SECURITY

The continuous evolution of threats and efforts to improve security are some of the factors that have characterized the state of cloud application layer security [21]. A detailed literature analysis has revealed several key findings that can help enhance the understanding of this domain.

Due to the rising number of attacks on web-based applications, their security is becoming more critical. Among the most common threats affecting these services' operations are DDoS, SQL injection, and CSRF. In addition to these, other attacks such as session hijacking are also becoming more prevalent. Even though there have been various steps taken to improve cloud application security, it is still a primary target for attackers. An attack on this layer can lead to various severe consequences, such as the loss of sensitive data or the disruption of services. To effectively address these issues, the cloud platform should have a robust security strategy [22].

Another challenge that cloud applications face is the compliance with regulations and privacy policies. Due to the various regulations introduced by the Health Insurance Portability and Accountability Act, GDPR, and CSPA, organizations are required to implement various measures to ensure the security of their customers' information. Non-compliance can result in costly penalties and reputational damage.

To address these issues, cloud applications [23] have started to adopt best practices and implement advanced security measures. These include the use of multi-factor authentication, encryption techniques, and secure coding practices. In addition to these, other measures such as the use of firewalls and RASPs have also been implemented to minimize the risks associated with attacks.

One of the most important steps that organizations can take to improve their cloud application security is by conducting regular security audits. This process can help them identify and prevent potential threats. With the help of advanced threat detection tools, they can also respond quickly to incidents to ensure the availability of their services [24].

In the future, research programs related to the security of cloud applications will focus on identifying and preventing new threats, developing effective mitigation techniques, and adapting to the changes brought about by the evolution of attack vectors and technologies. The collaboration between academic and industry researchers, as well as cybersecurity experts, will help develop innovative solutions that can help protect cloud-based services [25].

THREATS AND SOLUTIONS:

The section covers the various threats that can affect the cloud computing environment. It investigates a wide range of vulnerabilities, including XSS, SQL injection, CSRF, and DDoS attacks. It also explores other sophisticated threats, such as session hijacking and man-in-the middle attacks. These attacks take advantage of the weaknesses in the application layer' s design and functionality, which can expose the integrity and security of cloud-based services to significant risks.

A comprehensive approach is needed to combat these threats. The literature presents a variety of countermeasures that can be used to protect data-at-rest and in-transit. One of the most important components of this strategy is encryption. This method can prevent unauthorized access to the data. Another component of this strategy is to enhance the security posture by implementing MFA.

When it comes to enhancing cloud-based applications' security, it is important to implement secure coding techniques. This can help prevent the exploitation of various vulnerabilities, such as buffer overflows and injection attacks. Besides this, the use of runtime and application firewalls can also help prevent the spread of harmful activities.

Regular audits and continuous monitoring are also important factors that can help identify and prevent the exploitation of various vulnerabilities in the application layer. With the help of security analytics and advanced threat detection tools, organizations can now detect anomalous behavior and possible breaches in real-time, which can help minimize the impact of such incidents.

One of the most important factors that can affect the security of cloud computing is the adherence to regulatory standards such as the HIPAA, the General Data Protection Regulation (GDPR), and the Code of Conduct for Cloud Computing (CCPA). This ensures that organizations have the necessary policies and procedures in place to protect the privacy and security of their data.

Due to the evolution of cloud computing, the security of applications at the application layer is expected to undergo significant changes. This will allow researchers and practitioners to develop effective solutions that can address the unique challenges of this environment. Through collaboration among industry, academic, and cybersecurity groups, the goal of this project is to create novel and innovative security methods tailored for cloud-based environments.

To effectively address the security challenges of cloud computing, organizations should adopt a proactive approach. This can help them ensure the availability of their services, maintain confidentiality, and avoid exploitation of various vulnerabilities.

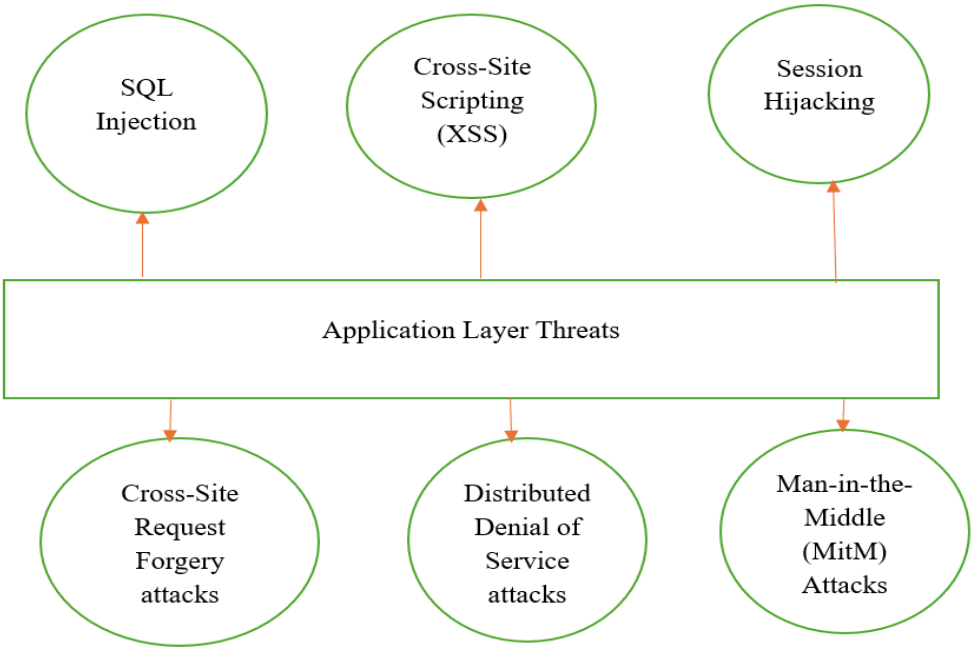

Figure 1. Threats Faced by Application Layer in Cloud Computing

BEST PRACTICES AND FUTURE DIRECTIONS:

The Best Practices and Future directions section aims to provide recommendations on how to improve the security of cloud computing. This section draws upon the findings of a survey and a literature review to provide guidance for researchers and practitioners. The section also explores best practices that can help improve the security posture of an organization's application layer. Some of these include implementing strong encryption techniques, establishing multi-factor authentication, and enforcing secure coding rules.

These recommendations can help organizations develop and implement policies that can meet the specific needs of their cloud computing environment [26].

In addition, this section explores the various directions that will be pursued in the field of cloud computing security. These include studying new methods for detecting and preventing threats, like the use of AI and machine learning [27], [28], as well as developing standards for assessing and improving the security of cloud applications.

Future research programs will also explore the integration of various innovative technologies, such as homomorphic encryption and blockchain, into cloud computing to enhance the security of applications. Researchers can develop novel ways to address issues related to data privacy, trust, and integrity in such environments [29].

The increasing collaboration among cybersecurity experts, academic institutions, and industry professionals will help drive innovation and improve the cloud computing security field. Through joint research programs

that combine the expertise of different disciplines, such as cybersecurity, computer science, and cloud computing can lead to effective solutions and insights [30].
The Future Directions and Best Practices section provides guidance and recommendations on how to enhance cloud computing's application layer security. It also highlights potential research opportunities. Adopting best practices and promoting innovation can help organizations enhance their cloud computing defenses against cyber threats.

CONCLUSIONS:

The paper thoroughly explored the security concerns of application layer in cloud computing. It highlighted the importance of safeguarding sensitive information and ensuring the integrity of the operations of the cloud. By identifying the key threats and developing countermeasures, the paper has provided guidance to help practitioners defend against these threats. This paper discusses the importance of maintaining regulatory compliance and adopting best practices, such as multi-factor authentication and encryption, to improve cloud security. It is important to prevent unauthorized access to your data. As organizations expand their operations and adopt cloud computing, they will need to collaborate and share knowledge and best practices to address the various security challenges that can arise in this new environment. Doing so will allow them to confidently manage their operations in an evolving digital world.

REFERENCES:

1. Mohamed, Saleh, Oluwaseyi, Joseph, & Robert, Abill. (2024). Evaluating the Development and Significance of Cloud Computing: Transforming the Digital Society. Journal of Cloud Computing.
2. Bello, S. A., Oyedele, L. O., Akinade, O. O., Bilal, M., Delgado, J. M. D., Akanbi, L. A., Ajayi, A. O., & Owolabi, H. A. (2021). Cloud computing in construction industry: Use cases, benefits and challenges. Automation in Construction, 122, 103441. https://doi.org/10.1016/j.autcon.2020.103441.
3. Sudha, K., & Nagamalai, J. (2021). A Review on Privacy Requirements and Application Layer Security in Internet of Things (IoT). Cybernetics and Information Technologies, 21(1), 50-72. https://doi.org/10.2478/cait-2021-0029.
4. Noman, H. A., & Abu-Sharkh, O. M. F. (2023). Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations. Sensors, 23(13), 6067. https://doi.org/10.3390/s23136067.
5. Mehmood, Asif, & Abbas, Asad. (2023). Safeguarding Sovereignty: Fortifying Data Security Measures for Confidentiality and Trust.
6. Dewang, Rupesh, Yadav, Mahendra, Awasthi, Surbhit, Raj, Om, Mewada, Arvind, & Bawankule, Kamlakant. (2023). Data secure application: An application that allows developers to store user data securely using blockchain and IPFS. Multimedia Tools and Applications, 83(1), 1-27. https://doi.org/10.1007/s11042-022-13252-y.
7. Lee, Chul Ho, Geng, Xianjun, & Raghunathan, Srinivasan. (2016). Mandatory Standards and Organizational Information Security. Information Systems Research, 27(1), 10-1287. https://doi.org/10.1287/isre.2015.0607.
8. Swamy, S. N., et al. (2017). Security threats in the application layer in IOT applications. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 477-480. https://doi.org/10.1109/I-SMAC.2017.8058316.
9. Brightwood, Seraphina, & Ariah, Success. (2024). Implementing Robust Security Measures in Cloud Infrastructure: Strategies, Best Practices, and Emerging Trends.
10. Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. Future Internet, 12(3), 55. https://doi.org/10.3390/fi12030055.
11. Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. Sensors, 20(13), 3625. https://doi.org/10.3390/s20133625.
12. Rahman, R. A., & Shah, B. (2016). Security analysis of IoT protocols: A focus in CoAP. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), 1-7. https://doi.org/10.1109/ICBDSC.2016.7460397.
13. Mahmood, K., & Javaid, N. (2020). Machine Learning Techniques for Securing IoT Applications: A Survey. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3024034.
14. Abbasi, M., Plaza, M., Prieto, J., & Corchado, J. (2022). Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions. IEEE Access. https://doi.org/10.1109/ACCESS.2022.3205351.
15. Ethan, Amelia, & Khan, Konal. (2023). Security Challenges in Cloud Computing: A Comprehensive Overview.
16. Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., Cordeiro, L., Diego, F., Sorokin, P., & Girolamo, D. F. (2023). Security in Cloud-Native Services: A Survey. Journal of Cybersecurity and Privacy, 3(4), 758-793. https://doi.org/10.3390/jcp3040042.

17. Nebbione, G., & Calzarossa, M. (2020). Security of IoT Application Layer Protocols: Challenges and Findings. Future Internet, 12(3), 55. https://doi.org/10.3390/fi12030055.
18. Lalit, Mohit, et al. (2022). IoT Networks: Security Vulnerabilities of Application Layer Protocols. 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 1-5. https://doi.org/10.1109/MACS.2022.9873967.
19. Kampars, J., Tropins, D., & Matisons, R. (2021). A Review of Application Layer Communication Protocols for the IoT Edge Cloud Continuum. 2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), 1-6. https://doi.org/10.1109/ITMS.2021.9568683.
20. Pandey, A., et al. (2012). Security of Cloud Computing Environments. International Journal of Computer Science and Information Technologies (IJCSIT), 3(6), 5369-5373.
21. Adeola Agbonyin, Premkumar Reddy, Anil Kumar Jakkani, Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES), International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp. 182-191. doi: https://doi.org/10.17605/OSF.IO/QX3DP
22. Jhurani, Jayesh & Reddy, Premkumar & Choudhuri, Saurabh Suman. (2023). FOSTERING A SAFE, SECURE, AND TRUSTWORTHY ARTIFICIAL INTELLIGENCE ECOSYSTEM IN THE UNITED STATES. International journal of applied engineering and technology (London). 5. 21-27.
23. Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a Novel Deep Learning Methodology for IOT Botnet based Attack Detection." International Journal on Recent and Innovation Trends in Computing and Communication Design 11 (2023): 4922-4927.
24. Saurabh Suman Choudhuri, et al. (2023). Navigating the Landscape of Robust and Secure Artificial Intelligence: A Comprehensive Literature Review. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 617–623. https://doi.org/10.17762/ijritcc.v11i11.10063
25. Premkumar Reddy, Yemi Adetuwo and Anil Kumar Jakkani, Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks, International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp.25-34. doi: https://doi.org/10.17605/OSF.IO/52RHK
26. Saurabh Suman Choudhuri, et al. (2023). Privacy-Preserving Techniques in Artificial Intelligence Applications for Industrial IOT Driven Digital Transformation. International Journal on Recent and Innovation Trends in Computing and Communication, 11(11), 624–632. https://doi.org/10.17762/ijritcc.v11i11.10064
27. Jhurani, Jayesh. (2023). Achieving Zero Day Close with Workday Artificial Intelligence (AI): Efficiency and Strategic Decision Making. IJARCCE. 12. 184-189. 10.17148/IJARCCE.2023.121127.
28. Choudhuri, Saurabh Suman, William Bowers, and Mohammad Nabeel Siddiqui. "Machine learning for pain point identification based on outside-in analysis of data." U.S. Patent No. 11,763,241. 19 Sep. 2023.
29. Gupta, Neha, et al. Fundamentals Of Chat GPT For Beginners Using AI. Academic Guru Publishing House, 2024.
30. Choudhuri, Saurabh Suman. "THE ROLE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN CRISIS MANAGEMENT." Redshine Archive (2024).