International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cloud Computing in Threats and Preventation

Devendra Sadeshwar, Aditya Bawankar

G H Raisoni University, Amravati, Maharashtra, India

Abstract

Cloud computing has revolutionized the current information technology infrastructure in the sense that it allows organizations to access various computing resources like storage, servers, database services, and applications through the internet in a flexible manner. However, the increasing trend of using cloud computing services has also given rise to various security risks. Some of the security risks associated with cloud computing services are data breaches, hijacking, insecure interfaces, denial of service, insider hijacking, and resource misconfiguration. This research paper discusses the various security risks associated with cloud computing services and the prevention strategies that can be adopted to avoid these risks. Some of the security risks associated with cloud computing services are data breaches, hijacking, insecure interfaces, denial of service, insider hijacking, and resource misconfiguration. The purpose of the present research is to identify the major security risks involved in cloud computing, as well as the preventive measures that can be taken to reduce the risks involved in it. The research is based on secondary research, where authentic information has been collected from reliable sources such as research journals, academic publications, cybersecurity publications, government publications, and international security publications. Several authentic publications were studied to gather detailed information regarding the risks involved in cloud computing. The research has pointed out a number of key threats that are a major issue in cloud environments. The threats include data breaches, DDoS attacks, insider threats, account hijacking, insecure APIs, malware injection, and cloud resource misconfiguration, among others. The research has pointed out that data breaches are a major threat in cloud environments because data is vulnerable to being compromised if the authentication mechanisms are inadequate or if the access control measures are inadequate. DDoS attacks are a major threat because, in such cases, the cloud resources are overwhelmed with traffic, causing service unavailability. Insider threats are a major issue in cloud environments because employees may misuse their privileges.

A part from that, the study also looks at the underlying vulnerabilities that make the cloud vulnerable to attacks. The vulnerabilities discussed in the study include weak password management, lack of encryption, poor identity management, unpatched software, technology risks, and monitoring mechanisms. The research study indicates that most security issues in clouds are not only caused by sophisticated cyber attacks but also due to human error In order to address the aforementioned risks, the research has examined different preventive measures that can be employed in the field of cloud security. These measures include different encryption techniques for the protection of the data, multi-factor authentication, identity management systems, firewalls, intrusion detection systems, firewalls, and the implementation of international security standards. The research has also highlighted the significance of implementing a multi-layered security system that comprises both proactive and reactive measures. Proactive measures are those that can protect the system from attacks before the attacks take place, whereas reactive measures can protect the system after the attack has already taken place.

KEYWORDS*: Cloud Computing, Cloud Security, Cybersecurity, Data Breach, Data Privacy, Data Integrity, Data Confidentiality, Distributed Denial of Service (DDoS), Account Hijacking, Malware Injection, Insecure Application Programming Interfaces (APIs), Insider Threats, Cloud Resource Misconfiguration, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Access Control Mechanisms, Data Encryption (At-Rest and In-Transit), Risk Assessment and Management, Security Controls, Intrusion Detection Systems (IDS), Firewall Protection, Shared Responsibility Model, Cloud Infrastructure Security, Security Governance, Compliance Standards, Vulnerability Assessment, Threat Detection and Prevention, Security Auditing, Proactive and Reactive Security Measures.*

1. Introduction

Cloud computing is arguably one of the most revolutionary technologies in the field of information technology. Cloud computing offers a wide range of opportunities for individuals and organizations to access computing resources, servers, storage, databases, networking, and software applications through the internet [1].Unlike traditional computing technologies, which demand huge investments, cloud computing offers a cost-efficient solution. Many businesses, regardless of their size, are increasingly using cloud computing as a means of improving their operations. Cloud services are basically divided into three types: Infrastructure as a Service, Platform as a Service and Software, as a Service [4]. These Cloud services let users pick what they need. Cloud services have ways to set them up like public Cloud services, private Cloud services, hybrid Cloud services and community Cloud services. This means Cloud services can give levels of security and access to organizations based on what the organizations need from Cloud services [2]. Major cloud service providers like Amazon Web Services, Microsoft Azure, and Google Cloud Platform are also very important for providing safe and reliable clouds to the world. Despite the various advantages associated with the adoption of cloud computing, various security risks are associated with the approach. To begin with, the fact that cloud computing uses the internet and that

data is stored in remote locations makes it a potential target for cybercriminals. Some of the security risks associated with the adoption of the approach include data breaches, hijacking, insecure interfaces, denial of service, insider, and misconfiguration risks [2][6].The shared responsibility model makes the security risks associated with the approach even higher, given that both the service providers and the consumers are responsible for the security of the data and applications [2][13].

As the number of organizations moving their critical data and applications into the cloud continues to grow, security is no longer a choice, but a necessity. it's a security issue may cause serious problems for the organization, including economic losses, tarnishing the image of the company, and losing the trust of customers. Due to these risks, companies should not take cloud security lightly. They are should take the right measures, including authentication systems, data encryption, and employee training [8],[15]. If the organizations are aware of the possible risks of cloud computing, they will be able to use a cloud computing without the fear of security failures and breaches by implementing the right measures to avoid these risks.

This research seeks to examine the risks of cloud computing in detail and present appropriate measures for creating a safe and sound cloud environment. Although cloud computing offers numerous advantages, it also raises serious security concerns for organizations. Since data and applications are stored on distant servers, which can be accessed only over the internet, there is always a threat of cyber-attacks on data and applications. Organizations have to put their trust in other organizations providing cloud services, which again raises concerns about the security of data, as data integrity, availability, and confidentiality become serious concerns for organizations. In addition to these threats, weaknesses in authentication, access control, cloud resource configuration, software vulnerabilities, and application programming interface security also pose a threat to security. Most security attacks are not only a result of advanced hacking techniques but also occur because of human error and a lack of proper security awareness. Hence, to ensure proper cloud security, a mix of all these factors is required [12].cloud computing plays a crucial role in digital transformation, but for its successful implementation, security management plays a vital role. Therefore, since cyber threats are constantly evolving, it is imperative for organizations to continually improve their security practices to ensure a secure, reliable, and trustworthy cloud computing environment, and this research has demonstrated the importance of identifying potential risks and implementing the necessary prevention mechanisms [13].

The purpose of this research is to examine the major threats that are involved in cloud computing and the prevention mechanisms that are adopted in order to curb these risks. In this regard, the aim of this particular study is to create a clear understanding of the cloud security challenges that are involved in cloud computing and the possible solutions that are adopted to curb these challenges, as revealed in the literature, research articles, and security reports. At the same time, this study reveals the importance of adopting the appropriate security measures in order to create a secure and sound cloud computing environment.

In the above context, it is clear that cloud computing is a new technology that offers several benefits in terms of its technological and economic benefits. At the same time, this technology is involved in several security challenges that are to be addressed with proper care. In this regard, it is essential to have a clear understanding of the cloud security risks that are involved in cloud computing in order to adopt the appropriate prevention mechanisms in the cloud computing environment.

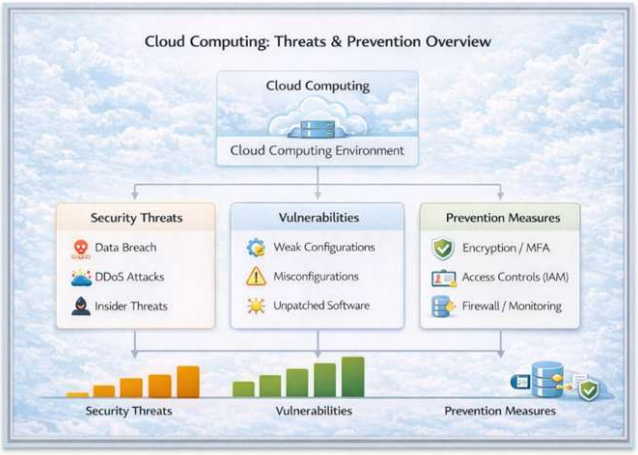

Fig.1. Cloud Computing: Threats & Prevention

2. Literature Review

One of the most widely is used to technological advancements in the recent past is a cloud computing. It's provides flexibility, scalability and cost of efficiency to businesses of all sizes. Nevertheless, with these advantages, there have also been a concerns regarding of security and privacy. Various studies they have emphasized that data security is the first challenge in cloud computing. It has also been pointed out that due to shared infrastructure, access, and third-party management, security risks such as data breaches, insider threats, APIs, and misconfigurations are affecting public as well as private cloud computing[5][10].

Some other researchers have also emphasized the significance of proper and efficient encryption technologies and identity management tools to ensure the security of critical data stored on the cloud. It has been revealed through various studies that an organization can minimize its vulnerabilities by implementing multi-factor authentication and access control technologies, as well as conducting periodic security audits. Various reports of the industry also support this fact, highlighting security incidents that have taken place due to weak passwords, improper configurations, and lack of monitoring. All of these sources also emphasize that, apart from technology, proper policies, employee education, and risk management strategies are also important. Moreover, various literature has also discussed different models of cloud computing, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), along with their differences, including security . It has been revealed through various researchers that, although the security of the infrastructure is the responsibility of the cloud service providers, users are also responsible for ensuring the security of their data [12].

Researchers have highlighted that one of the key challenges with the adoption of cloud computing is the issue of security. Initial studies on the security of the cloud identified the key concern with the confidentiality, integrity, and availability of data. The researchers identified that the key concern with the adoption of the cloud was that it involved the use of

third-party service providers. This meant that users did not have control over their data. This was identified as one of the key challenges with the adoption of the cloud. Studies have identified that one of the key challenges with the adoption of the cloud was the issue of data breaches [2][10]. Unauthorized access of data was identified as one of the key challenges with the adoption of the cloud. There have been various research publications on Distributed Denial of Service (DDoS) attacks, which have been cited as one of the biggest threats to cloud services and their availability. According to various cybersecurity reports, in DDoS attacks, botnets send excessive traffic to cloud servers, resulting in disruptions to cloud services. The research has proposed filtering of cloud traffic, balancing of cloud services, and monitoring of cloud services as countermeasures for DDoS attacks[2][10].

Similarly, the issue of insider threats has been extensively researched in cloud security research studies. It has been observed in academic research studies that insiders, such as employees or contract workers with authorized access, can cause harm to cloud environments, both intentionally and unintentionally [8]. The importance of implementing a strict access control policy, role-based access management, and training employees has been emphasized in research studies for minimizing the potential risks caused by insiders [15]. The importance of implementing the principle of least privilege has been emphasized in multiple research studies. Encryption methods have been extensively discussed in the context of cloud security, and it has been emphasized as a key preventive measure in cloud security. According to various researchers, the implementation of robust encryption for data in transit and in rest can greatly mitigate the chances of cyber attacks [12]. Additionally, multi-factor authentication and Identity and Access Management have been proposed to enhance the security of authentication and access control. Comparative studies have been conducted to reveal that the number of successful cyber attacks on organizations using multi-layered security models is lower compared to those using single-layer security models [6][11].

Literature has also pointed out the shared responsibility model in cloud security. The shared responsibility model is a concept in cloud security that implies that the responsibility for cloud security is shared between cloud service providers and consumers. While cloud service providers are responsible for providing security in the cloud, consumers are responsible for the configuration, data, and user access management in the cloud. It has been indicated that a lack of understanding of the shared responsibility model is a potential security threat.Recent research has been focused on providing proactive security measures in cloud security, rather than reactive security measures. The research has indicated that predictive threat analysis, artificial intelligence, and automated response systems are potential research directions in cloud security in the future. The application of machine learning has been indicated as a potential advanced measure in cloud security for detecting anomalies in cloud systems [2] [6].

3. Research methodology

3.1. Cloud computing and threats and prevention Research process.

When it came to studying the various threats associated with cloud computing and the ways in which they could be prevented, we did not conduct any experiments but rather utilized the resources we had to obtain the information we needed. To obtain the information we needed about the various threats associated with cloud computing and the ways in which they could be prevented, we studied information from the following sources: A Research journals: We read various articles published in journals focused on cloud computing and cybersecurity to obtain information about the various things experts in the field had discovered. Industry reports: We obtained reports from various cybersecurity organizations, such as the Cloud Security Alliance, which provided us with information about the various things we needed to be aware of. Security documents: We obtained security information from various organizations, such as Amazon Web Services, Microsoft Azure, and Google Cloud, to obtain information about the ways in which they kept their platforms secure. Instead of focusing on the numbers or the statistics, we pieced together the information to provide a picture of the current threats and security strategies. In the following section, I will provide a flowchart that describes the basic steps that our research process followed: identifying the sources, collecting the data, analysing the information, and drawing conclusions to help improve the security of the cloud [2] [6].

Finally, the research process is concluded with the interpretation of the gathered findings and the formulation of useful insights related to cloud security measures. By examining the relationship between threats and prevention measures, the research aims to emphasize the significance of using effective security measures for cloud computing environments. The research findings of this study will help organizations, students, and researchers understand the security issues of cloud computing and how they can be tackled using effective measures. Overall, the research process offers a systematic way of conducting research in the field of cloud computing threats and the mechanisms for their prevention. This study contributes to the enhancement of the level of awareness about the security risks associated with cloud computing and the need to adopt appropriate security practices for the provision of secure cloud computing services.

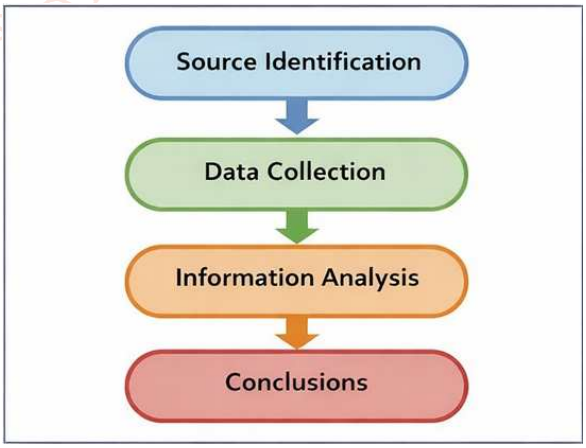

Fig.2. Research Process Diagram

it's above diagram of the research process clearly explains the methodology adopted in the study. The first step in the research process is Source Identification, in which reliable academic journals, industry reports, and official cloud documentation related to the security of cloud computing are identified. The second step in the research process is Data Collection, in which relevant information from the identified sources is collected. this third step in the research

process is Information Analysis, in which the collected data is analysed to a identify the common risks, patterns, and best practices in the security of cloud computing. Finally, in the last step of the research process, the findings are concluded in the form of suggestions in the Conclusion step [1] [6].

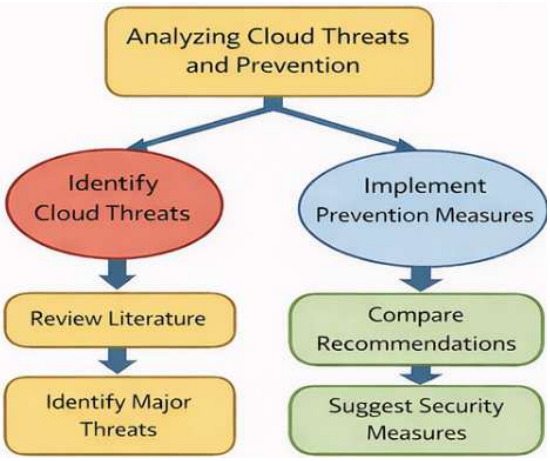

Fig.3. Approach to analyzing cloud Threats and Preventation.

This section presents an overview of the methodical approach to cloud computing threats analysis and prevention. The information was obtained through relevant journals, reports, and official cloud documentation. The data was further studied to establish the most common security threats. The security threats identified in the research include data breaches, unauthorized access, misconfigurations, and other security threats in cloud computing. Through the analysis of multiple reliable sources, the research identified the security threats that are most common in cloud computing scenarios. In addition to security threats, the research also identified the recommended security measures to prevent these identified threats. Various security measures such as encryption, multi-factor authentication, monitoring, and configurations were studied. The aim was to associate these security measures with the identified security threats [5] [10].

3.2. Data Collection

The type of data employed in this study is collected from secondary sources. Secondary data refers to published research papers, government publications, journal articles, books, and official security guidelines. Reliable sources like NIST publications, Cloud Security Alliance (CSA) reports, ENISA reports, and research journals were consulted during the collection of data [1][15]. The data collection procedure was conducted in three phases. In the first phase, relevant keywords such as "cloud computing security threats," "data breach in cloud," and "cloud security prevention mechanisms" were employed to search research journals and official websites. In the second phase, selected articles and reports were analysed to gather valuable information about threats and their preventive measures. In the final phase, the gathered information was compiled on the basis of categories such as threat types and related security controls. Only authentic and recognized sources were taken into consideration to ensure the correctness and authenticity of the study. Obsolete and unauthentic sources were not considered to ensure quality and accuracy.

3.3. Data Analysis

The collected data was then analysed through a comparative and conceptual analysis approach. The primary objective of the data analysis was to determine the patterns of various threats and the security measures used to counter them. Each threat was separately analysed to determine: How the threat impacts cloud infrastructure Which vulnerabilities are exploited by the threat Which preventive measures are most effective [14]. For instance, the risks is associated with data breaches were are analysed together with the measures of the encryption and access control. In a similar manner, DDoS threats were analysed together with firewalls and traffic monitoring systems By contrasting various research findings, the study determines the most effective recommendations for prevention. The analysis also aims to determine the nature of the preventive measures, whether proactive (preventing attacks before they occur) or reactive (mitigating the impact after an attack has occurred).

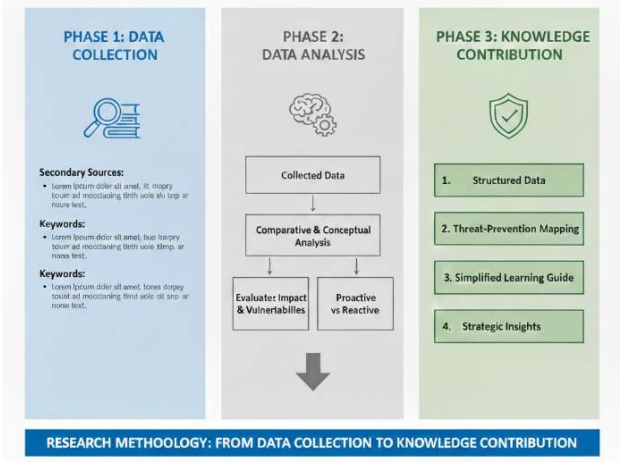

Fig.4. from Data Collection to Knowledge Contribution.

3.4. Data Contribution

This research contributes to the structuring of unorganized data related to the cloud computing threats and their prevention methods. Unlike focusing on a single type of attack, this research provides a clear insight into the different threats and connects them to the relevant security methods. The threat prevention mapping diagram developed in this research work helps to represent the relationship between the threats and their prevention methods[2][10]. This can help students, researchers, and small-scale organizations understand the concepts of cloud security in a clearer way. Although this research work is theoretical in nature, it provides a clear insight into organizations to improve their cloud security methods.

4. Result

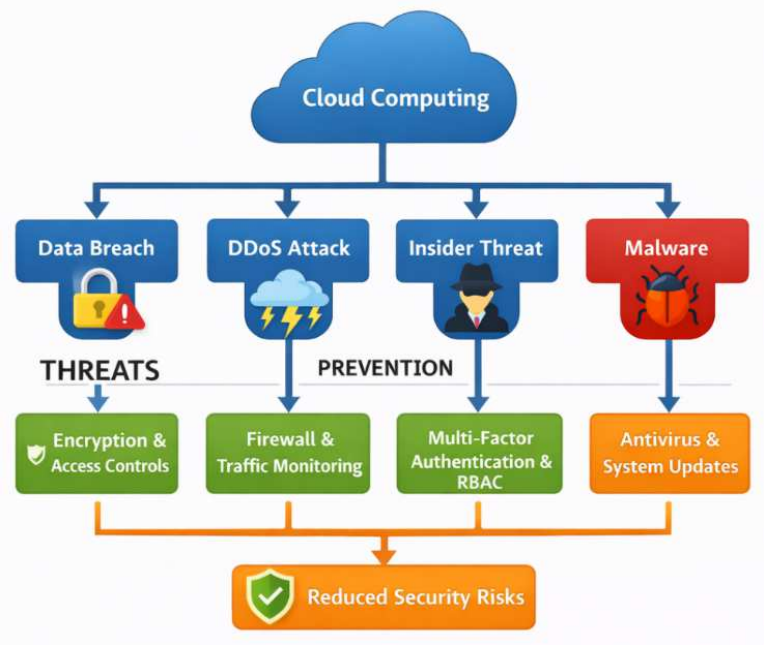

Fig.5. Cloud Security Threat–Prevention Result Model.

5. Conclusion

In conclusion, it can be stated that cloud computing technology has changed the way organizations store and manage their data and access it. At the same time, it can be noted that this technology, along with its advantages, poses a great security concern to the organizations that adopt it [3]. The present study discussed various security issues that occur in cloud computing technology, such as security breaches, unauthorized access, and insider attacks. From the study, it can be noted that cloud computing technology needs to be monitored and security measures implemented to protect it [7].It can be noted that various security solutions play a significant role in protecting cloud computing technology and that it is very important to understand the responsibility that an organization needs to take along with the cloud service providers to protect the technology completely.

This study aimed to identify the major security issues related to cloud computing and assess the effectiveness of different measures taken for prevention. This study verifies that cloud security is a major concern for organizations, service providers, and individuals. The major security risk related to cloud computing is data breach, which may cause financial loss, damage to reputation, and legal consequences. Data breaches can occur because of a weak authentication process, incorrect configuration of storage services, or human error [10]. Cloud computing services store a huge amount of data, and if there is a slightest security risk, it can cause a huge impact. Another significant threat identified by this research is Distributed Denial of Service (DDoS) attacks [9]. DDoS attacks on the availability of cloud services occur when an attacker sends an unwanted surge of traffic to a server, resulting in a denial of service. Despite the fact that cloud service providers have enhanced traffic filtering systems, the dynamic nature of DDoS attacks continues to challenge these systems. Ensuring availability is a critical aspect of cloud security management [2][13].

References

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology (NIST), Special Publication 800-145, (2011).

[2] Cloud Security Alliance, "Top Threats to Cloud Computing: Egregious Eleven," CSA Report,(2019). https://cloudsecurityalliance.org/research/top-threats/

[3] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58,(2010). https://doi.org/10.1145/1721654.1721672

[4] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp.1–11,(2011).

[5] https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[6] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592,(2012).

[7] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An Analysis of Security Issues for Cloud Computing," Journal of Internet Services and Applications, vol. 4, no. 1,(2013).

[8] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality," Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616,(2009).

[9] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, (2009).

[10] ENISA, "Cloud Computing Risk Assessment," European Union Agency for Cybersecurity Report,(2019).

[11] N. Gonzalez et al., "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud

Computing," Journal of Cloud Computing, vol. 1, no. 1,(2012).

[12] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," IEEE Cloud Computing,(2010).

[13] Y. Chen and R. Sion, "On Securing Untrusted Clouds with Cryptography," ACM Workshop on Cloud Computing Security,(2010).

[14] J. Rittinghouse and J. Ransome, Cloud Computing: Implementation, Management, and Security, CRC Press,(2017).

[15] ISO/IEC 27001, "Information Security Management Systems – Requirements," International Organization for Standardization,(2013).

[16] National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," NIST SP 800-53,(2020). Available at:https://doi.org/10.6028/NIST.SP.800-53r5