Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 6, Issue 1, 2026 (pp. 28-40)
www.abjournals.org

ENHANCING SECURITY IN CLOUD COMPUTING ENVIRONMENT

Abubakar Jibrin[1] and Aliyu Sani Ahmad[2].

[1&2]Department of Computer Science, Faculty of Computing and Information Science, Federal University Wukari, Taraba State, Nigeria.

Emails: [1]jibson.abu555@yahoo.com; [2]alally_ahmad@yahoo.com

Cite this article:

Abubakar Jibrin, Aliyu Sani Ahmad (2026), Enhancing Security in Cloud Computing Environment. Advanced Journal of Science, Technology and Engineering 6(1), 28-40. DOI: 10.52589/AJSTE-BUIU5R07

Manuscript History

Received: 21 Dec 2025

Accepted: 18 Feb 2026

Published: 5 May 2026

ABSTRACT: *Cloud computing is the most emerging technology that becomes the demanding architecture for IT enterprise. It exhibits remarkable potential to offer cost-effective and more flexible service to the customers over the network. A vast number of big organisations like Google, Facebook, Dropbox etc. all depend upon this type of computing. It dynamically increases the capability of the organisation without training new people. Cloud computing moves its database and applications to various data centres across various countries where management of data and its security is the major concern. The dynamic and scalable nature of cloud computing creates security challenges in their management examining policy failure or malicious activity. In this paper, we examine the detailed design of cloud computing architecture in which service models, deployment models, cloud security are exploded. Furthermore, this study identifies the security challenges in cloud computing during the transfer of data into the cloud and provides a viable solution to address the potential threats.*

KEYWORDS: Enhancing, Security, Cloud, Computing, Environment, Challenges.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 6, Issue 1, 2026 (pp. 28-40)

www.abjournals.org

INTRODUCTION

With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful and more universally available than ever before. This technological trend has enabled the realisation of a new computing model called cloud computing, in which resources (e.g. CPU and storage) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. In the last few years, different business companies increasingly understand that by tapping the cloud resources and gaining fast access, they are able to reduce their initial business cost by paying only the resources they used rather than the need of potentially large investment (owning and maintenance) on infrastructure. Rapid deployment, cost reduction, and minimal investment are the major factors to employ cloud services that drive many companies [1][2]. Cloud computing is explained by the National Institute of Standard and Technology (NIST). It is a model to enable convenient, ubiquitous and on-demand network access that is the configurable computing resources to shared resources which can be delivered and provisioned rapidly with minimum managerial interaction [3]. Many companies like Microsoft, Google, Amazon, IBM, among others, developed cloud computing systems and provided a large number of customers by enhancing their services [4]. The advantages of using cloud computing are offering infinite computing resources, low cost, security controls, hypervisor protection, rapid elasticity, high scalability and fault tolerant services with high performance. Moreover, there are significant barriers to adopting cloud computing like security issues regarding privacy, compliance and legal matters because it is a relatively new computing model having a great deal of uncertainty regarding the security of all levels, such as host, network, data levels, and application[5]. The management of data and services is an important concern when the databases and application software are moved from the cloud to the large data centres. There may arise many security challenges regarding the use of cloud computing including the privacy and control, virtualization and accessibility vulnerabilities, credential and identity management, confidentiality, authentication of the respondent device and integrity [6][7]. Cloud computing is authorised through the virtualization technology in which the host system operates an application referred as a hypervisor that generates one or more Virtual Machines (VM) and it faithfully simulates the physical computers. These simulations can be able to operate any software from the operating system to the end-user application [8].

LITERATURE/THEORETICAL UNDERPINNING

The study starts by identifying cloud computing security challenges and their mitigation strategies from the literature. To identify cloud computing security challenges and their solutions, grey literature, systematic literature review, snowball sampling etc., could be used, but this report uses snowball sampling and literature review. Literature Review (LR) helps to identify state of art in a study and snowball sampling helps to revisit references used in the article and find information related to the current study.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 6, Issue 1, 2026 (pp. 28-40)

www.abjournals.org

Categories of Enhancing Security in Cloud Computing Environments

Cloud computing security is the major concern and has various challenges that need attention [51][14]. From the recent surveys on IT executives and CIO's conducted by IDC, it was clear that security was the highly cited (74%) challenge in the cloud computing field [9][29]. A comparison with grid computing systems also proves that for cloud computing security the measures are simpler and less secure [19]. Security in cloud computing is totally based on the cloud service provider, who is responsible for storing data and providing security [20].

Data

Data Security: Information from articles that discuss data security and data protection are considered. Security provided by cloud SP's might not be highly cost effective when implemented in small companies. But when two or more organisations share a common resource there is a risk of data misuse. In such a situation it is required to secure data repositories [36]. Not only the data repositories but also data should be secured in any stage such as storage, transit or process [33]. Since this kind of sharing resources is prevalent in the CC scenario, protection of data is important and is the most important challenge among other CC challenges [54][41][37].

Data Locality: Information from articles that discuss data locality, jurisdictional issues, risk of seizure and loss of governance are considered. Using CC applications or storages services questions such as "does CSP allow to control the data location?" arise and reason for asking this question is explained in this section [40]. We know that in CC the data can be hosted anywhere and in most cases the customer does not know the location of his data i.e., the data is generally distributed over a number of regions [38][29][35]. It is also known that when the geographical location of data changes the laws governing that data also change. This clarifies that the user's data (information, applications) that is stored in cloud computing (distributed over a number of regions) is affected by the compliance and data privacy laws of that country (whichever country user's data is located). So, it is necessary that the customer should be informed about the location his data is stored in the cloud [45].

Data Integrity: If a system maintains integrity, its assets can only be modified by authorised parties or in authorised ways. This modification could be on software or hardware entities of the system [55]. Data integrity in any isolated system (with a single database) can be maintained via database constraints and transactions. But in a distributed environment, where databases are spread out in multiple locations, data integrity must be maintained correctly, to avoid loss of data [34][35].

Data Segregation: Another issue in cloud computing is multi-tenancy. Since multi-tenancy allows multiple users to store data on cloud servers using different built-in applications at a time, various user's data resides in a common place. This kind of storage shows a possibility for data intrusion. Data can be intruded (malicious user retrieving or hacking into others data) by using some application or injecting a client code [45][23]. The user should ensure that data stored in the cloud should be separated from other customer's data [19][29][40].

Data Access: Information from articles that discuss data access, access rights, privileged user access, access control, administrative access are considered. This issue mainly relates to security policies. Policies are described as "conditions necessary to obtain trust, and can also

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

prescribe actions and outcomes if certain conditions are met" [39]. Every organisation has their own security policies. Based on these policies, employees will be given access to a section of data and in some cases, employees might not be given complete access. While giving access it is necessary to know which piece of data is accessed by which user [13][26].

Networking

Network Security: Information from articles that discuss network security and VPN network are considered. Data should not be leaked while transmission and it is one of the requirements in information security [42]. To prevent leakage of sensitive information while transferring, a strong traffic encryption technique such as Secure Socket Layer (SSL) and the Transport Layer Security (TLS) are required. Sensitive data are obtained from enterprises, processed by any service application and stored at the service vendor end.

Application Security: Information from articles that discuss web application security, API security, application vulnerabilities and application security are considered. With new advantages cloud also brings to the developers' novel vulnerabilities and threats related to APIs [11]. It is known that in the cloud, any application or software that is used lies in the cloud but not with the actual user and if this software/application has vulnerabilities then it can have a decremental impact on all the customers using the cloud [44][14][50]. If the insecure APIs are not secured the vulnerabilities that can lead to compromising security, can also lead to men in the middle of attacks and affect the availability of CC [52][53][43].

Host and Network Intrusion: This problem arises in PaaS, where control might be given to the user by SP to some extent. Service providers should keep in mind that control below the application level, such as host and network intrusion shall not be given to the user and the provider should maintain inaccessibility between applications [45]. By using programs such as trojan horses and malware which leak sensitive data can help intruders to gain access to sensitive information [41][29][22].

Denial of Service: Denial of service attacks are possible in the cloud which can be a threat to data under transmission [16][42][53] [36]. Unlike bypassing preventive and security measures the attacker uses methods such as packet splitting, payload mutation, shell-code mutation and duplicate insertion [21].

Men in Middle of Attack: Attackers create an independent connection which relies on the messages between user and provider. The attacker makes the user and provider believe that this connection is secured and makes them talk directly, but behind the scene the attacker controls the whole connection and receives every message which is sent between them (user and provider) [48][18][35]. The attacker can also possibly modify the message before sending it to the respondent [41].

Virtualization

Vulnerability in Virtualization: Information from articles that discuss vulnerability in virtualization and cross-vm information leakage are considered. The most commonly used multiple way to create multiple virtual machines on a single physical machine is done using Virtual Machine Monitor (VMM) approach. Hypervisors are also used to manage multiple VMs and any flaws in the hypervisors can allow attacker to gain access in an inappropriate

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

way, even when tools such as Xen access are used many security risks can be found, which allow admin to see through the user level process while the customer is running his VM and attacker can easily install a malicious code [32][17][36].

Virtual Machine Protection: Information from articles that discuss virtual machine protection and securing virtual machine boundaries are considered. Multiple VM's can be instantiated or halted in a single server (machine) to satisfy a list of services accepted. These services can also run multiple applications which are based on different operating system environments [15]. In relation to this author in [12] expressed his concern towards securing the boundaries of virtual machines. Since the virtual machines created in cloud server have virtual boundaries (unlike general isolation where multiple hard disk drives), it's the responsibility of CSP to ensure VM's that use common resources on the same physical server (i.e., CPU, memory, I/O, NIC and others) are separated [12].

Networking in Virtual Networks: Information from articles that discuss networking in virtual networks, networking problems, virtual management, virtual network security and hypervisor security are considered. Virtual machine instances interconnectivity (i.e., communication) is a huge concern in CC [25][17]. Traditional mechanisms such as VLAN's (Virtual Local Area Network) and firewalls are proving to be inefficient when used in a virtualized environment [24]. The security of a computer depends on the quality of underlying security mechanisms or kernels which control the execution of process [28].

Organisation

Organisational Security Management: When adapting to cloud computing, some changes are introduced to the security management, information security lifecycle models, even the corporate IT standards and policies need to be changed [49]. There are issues such as less coordination among different communities of interest within client organisations. The customer also has to face new risks introduced by a perimeter-less environment, such as data leakage due to multi-tenancy, issues like local disasters and provider's economic instability. But since the cloud computing environment is distributed in nature, re-evaluate best practices and adoption of secure cloud computing applications become extremely complex as they require well-structured cyber insurance [46].

Trust Management and Policy Integration: Trust is the key problem in the CC environment as CC is not completely trustable for users [50][42][22]. An organisation using a cloud computing application has to give some of its critical information to use certain services provided by the cloud service provider. This organisation needs to develop trust in remote execution/storage and placing sensitive data in the cloud is tough as the company feels that it is losing control over data and there is much less transparency in cloud [31][27][10][16]. Lack of this control is leading to distrust in CC [40].

Failure in Providing Security: Information from different articles that discuss fault tolerance and failure in providing security are considered. Failure in providing security to the infrastructure under control of the cloud provider can result in compromising subscriber's security. Even a single weak link in cloud computing can cause a security threat to multiple entities connected in it. For a customer to secure his data, he/she should believe in the service provider's security [47][30][18]. It is evident that customers must also have trust in provider

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

security. For a cloud to be trusted and considered strong, simple but yet important features such as logging, security policies, incident response, etc., should also be strong [32].

Identified Solutions

These identified solutions are suggestions from different authors and could vary from person to person or organisation to organisation. These solutions can be used individually or in combination to give better solutions for identified challenges.

Encryption: Encryption is suggested as a solution to secure information which is being transferred, stored (at rest) or under any other operation. This section maps to the challenges identified in the previous section and explains how these solutions can minimise the effect of challenges while using cloud computing. Access Rights: Data owners should give permission to a particular party so that they can access the data easily. To provide this data access control, a standard based heterogeneous data centric security is used to give data protection to applications for preventing problems [46].

Use of Central Global Transaction Manager: Usage of central global transaction manager refers to 2-phase commit protocol as per XA standards. As a mix of on-premise and SaaS applications can arise data integrity problems in the world of SOA and cloud computing (SaaS application's functionality usually gets exposed to XML based API's. In SOA, many on-premise applications expose functionality based on SOAP and REST web services protocols. There are standards available for data integrity in HTTP but are yet immature (WS-transaction and WS-reliability) [45][40].

Ensuring boundaries: SaaS ensures that there must be clear boundaries for individual user data. This boundary must be ensured not only on physical level, but also at application level to segregate the data from different users (solution to data segregation and data access) [45].

METHODOLOGY

Collecting Data from Literature Review: To identify which areas of cloud computing security need more research, initially CC challenges are found (this is done by searching the literature). Available methods for achieving this are literature review (LR) and systematic literature review (SLR). SLR is used to find all available data relevant to a particular research area [30]. Since the topic of cloud computing is a novel one, literature review and snowball sampling is employed [60]. The articles written by the researchers are based on scientific papers, online sources, journals etc. Snowball sampling revisits all these references used in writing an article. This in turn increases the final set of papers used to understand the problem (selected for study). In this context, since this study had the threat of finding fewer references, the authors chose snowball sampling.

Collecting Data from Real World: Based on results of literature review and empirical study, mechanisms that are actually used in organisations to handle the security challenges identified from literature are needed to be found. Other methods available under empirical studies are interviews, case studies, experiment and post-mortem. The interview is a process of gathering in-depth information to the interviewer's question from the responder.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 6, Issue 1, 2026 (pp. 28-40)

www.abjournals.org

Methods of Data Analysis: Several methods of data analysis can be proposed for enhancing security in cloud computing environments. These methods are aimed at extracting actionable insights from various data sources to identify security threats, detect anomalous behaviour, and mitigate risks effectively. Here are some proposed methods.

Log Analysis: Log analysis is a fundamental method of data analysis used in enhancing security in cloud computing environments. Logs are generated by various components of cloud infrastructure, including servers, networking devices, applications, and security tools. Analysing these logs can provide valuable insights into system activities, user behaviour, and security events.

Behavioural Analytics: Behavioural analytics is a method of data analysis that focuses on understanding and identifying patterns in user behaviour to detect anomalies and potential security threats. In the context of cloud computing security, behavioural analytics can be utilised to monitor user activities, identify deviations from normal behaviour, and detect suspicious actions that may indicate unauthorised access or malicious activity.

Network Traffic Analysis (NTA): Network Traffic Analysis (NTA) is a method of data analysis used to monitor and analyse network traffic patterns, identify anomalies, and detect potential security threats within a networked environment. In the context of enhancing security in cloud computing environments, NTA plays a crucial role in detecting and mitigating cyber threats, identifying malicious activities, and ensuring the integrity and confidentiality of data.

RESULTS/FINDINGS

The results of the systematic review are summarised in the Table above which shows a summary of the topics and concepts considered for each approach. As it is shown in the Table, most of the approaches discussed identify, classify, analyse, and list a number of vulnerabilities and threats focused on Cloud Computing. The studies analyse the risks and threats, often give recommendations on how they can be avoided or covered, resulting in a direct relationship between vulnerability or threats and possible solutions and mechanisms to solve them. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other issues related to security in the Cloud such as the data security, trust, or security recommendations and mechanisms for any of the problems encountered in these environments.

Security in the SPI Model

The cloud model provides three types ofservices

Software as a Service (SaaS): the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).

Platform as a Service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure his own applications without installing any platform or tools on their local machines. PaaS refers to providing platform layer resources, including operating system support and software development frameworks that can be used to build higher-level services.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Advanced Journal of Science, Technology and Engineering
ISSN: 2997-5972
Volume 6, Issue 1, 2026 (pp. 28-40)
www.abjournals.org

Infrastructure as a Service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Summary of the topics considered in each approach

Topics/References	[4]	[6]	[10]	[16]	[17]	[18]	[19]	[20]	[21]	[22]	[23]	[24]	[25]	[26]	[27]
Vulnerabilities		X		X	X	X	X	X	X			X			X
Threats		X		X	X	X	X	X	X	X	X	X	X	X	X
Mechanisms/Recommendations	X			X		X		X				X	X	X	X
Security Standards							X			X					
Data Security	X		X				X		X		X		X		X
Trust			X								X		X	X	X
Security Requirements	X		X						X		X			X	X
SaaS, PaaS, IaaS Security					X				X			X			

DISCUSSION

In this part, the suggested security solution discusses the challenges faced in the adoption of cloud computing environments that influence the customers to release security burden with trusting a third party. This study observed that the concerns of trust, security and privacy highlighted by many cloud providers and customers. The deployment of security strategies in the cloud environment to achieve integrity, confidentiality and availability of data or systems that adopt to change the relationship between the cloud provider and the customers. A trust-worthy access control infrastructure is needed to avoid any unauthorised access to the shared resources. Trust required operating in each layer of the cloud service models (IaaS, SaaS, PaaS) and it needs to ensure the security at the technical, legal, procedural and operational level to allow secure communication

IMPLICATION TO RESEARCH AND PRACTICE

Enhancing security in a cloud computing environment has several critical implications such as:

Data Protection and Privacy:

- **Confidentiality:** Improved security measures help ensure that sensitive data stored in the cloud is protected from unauthorised access.
- **Integrity:** Enhanced security helps maintain the accuracy and completeness of data, preventing unauthorised modifications.
- **Availability:** Security enhancements protect data and services from attacks that could lead to downtime, ensuring continuous availability.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Compliance and Legal Requirements:

- **Regulatory compliance:** Many industries are subjected to strict regulations regarding data security. Enhanced security helps organisations meet these requirements
- **Legal Protection:** Implementing strong security measures can protect organisations from legal repercussions in the event of a data breach.

Trust and Reputation:

- **Customer Trust:** Ensuring robust security measures can enhance customer confidence in using cloud services, leading to increased adoption and customer loyalty.
- **Brand Reputation:** Preventing data breaches and ensuring data security helps maintain a positive brand image avoids the negative publicity associated with security incidents.

Operational Efficiency:

- **Risk Mitigation:** Storage security practices reduce the data breaches, financial losses and operational disruptions.
- **Incident Response:** Enhanced security often includes better monitoring and incident response capabilities, allowing for quicker detection and mitigation of security incidents.

Cost implications:

- **Prevention of Financial Losses:** Investing in security can prevent costly data breaches and associated losses, including fines, legal fees and remediation costs.
- **Cost of Security Measures:** Implementing enhanced security measures require investment in technology personnel and processes.

CONCLUSION

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organisations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. We have presented security issues for cloud models: IaaS, PaaS, and IaaS, which vary depending on the model. As described in this paper, storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also targets for some attacks, especially when communicating with remote virtual machines.

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

FUTURE RESEARCH

Enhancing security in cloud computing environments involves a multifaceted approach that encompasses various technological, procedural and policy-based measures. Above are some key features and research areas focused on enhancing cloud security:

1. Encryption Technology
2. Identity and Access Management
3. Intrusion Detection and Prevention System
4. Data Loss Prevention
5. Incident Response and Forensics
6. Threat Intelligence Sharing
7. User Education Awareness

REFERENCES

[1] M. Armbrust, I. Stoica, M. Zaharia, A. Fox, R. Griffith, A. D. Joseph, R.
[2] Katz, A. Konwinski, G. Lee, D. Patterson, and A. Rabkin, "A review of cloud computing," Commun. ACM, vol. 53, no. 4, 2010.
[3] R. B. Bohn, J. Messina, F. Liu, J. Tong, and J. Mao, "NIST cloud computing reference architecture," Proc. IEEE World Congress. Serv., pp. 594–596, 2011.
[4] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Spec. Publ. 800-145, vol. 145, p. 7, 2011.
[5] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and privacy in cloud computing: A survey," Proc. 6th Int. Conf. Semant. Knowl. Grid, pp. 105–112, 2010.
[6] D. G. Rosado, R. Gomez, D. Mellado, and E. Fernández-Medina,
[7] "Security analysis in the migration to cloud environments," Futur. Internet, vol. 4, pp. 469–487, 2012.
[8] C. Wang, Q. Wang, K. Ren, and W. J. Lou, "Ensuring data storage security in cloud computing," 17th Int. Work. Qual. Serv., pp. 37–45, 2009.
[9] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, 2014.
[10] L. Savu, "Cloud computing deployment models, delivery models, risks and research challenges," Proceeding IEEE Int. conf. comput. manag., 2011.
[11] Security in the cloud. *Clavister White Paper*, 2010. cited By (since 1996) 1. 8, 25, 30, 36, 43, 54, 60, 63, 66, 70
[12] Imad M. Abbadi and Cornelius Namiluko. Dynamics of trust in Clouds— Challenges and research agenda. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, pages 110–115, 2011. 46
[13] Hussain Al-Aqrabi, Lu Liu, Jie Xu, Richard Hill, Nick Antonopoulos, and Yongzhao Zhan. Investigation of IT security and compliance challenges in security-as-a-service for cloud computing. In *Object/Component/ServiceOriented Real-Time Distributed*

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

Computing Workshops (ISORCW), 2012 15th IEEE International Symposium on, pages 124–129, 2012. 33, 37, 40, 44, 49, 75

[14] Aiiad Ahmad Albeshri and William Caelli. Mutual protection in a cloud computing environment. In *IEEE 12th International Conference on High Performance Computing and Communications (HPCC 2010)*, pages 641– 646, 2010. 11, 27, 33, 37, 46, 52, 62, 75

[15] Gabriel Antoniu. Autonomic cloud storage: challenges at stake. In *Complex, Intelligent and Software Intensive Systems (CISIS), 2010 International Conference on*, pages 481–481, 2010. 29, 35

[16] Aashish Bhardwaj and Vikas Kumar. Cloud security assessment and identity management. In *Computer and Information Technology (ICCIT), 2011 14th International Conference on*, pages 387–392, 2011. 24, 33, 37, 40, 49, 58, 72

[17] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, June 2009. 42

[18] Jianyong Chen, Yang Wang, and Xiaomin Wang. On-demand security architecture for cloud computing. *Computer*, 45(7):73–78, 2012. 38, 39, 46, 50, 52, 74, 75

[19] W. Dawoud, I. Takouna, and C. Meinel. Infrastructure as a service security: Challenges and solutions. In *2010 The 7th International Conference on Informatics and Systems (INFOS)*, pages 1–8. IEEE, March 2010. 32, 35, 37, 41, 42, 43, 44, 46, 50

[20] L. Ertaul, S. Singhal, and G. Saldamli. Security challenges in cloud computing. *California State University, East Bay. Academic paper http://www. mcs. csueastbay. edu/ lertaul/Cloudpdf*, 2009. 12, 15, 18, 27, 28, 33, 38, 39, 40, 47, 54, 56, 64, 65, 66, 67, 68

[21] Christoph Fehling, Thilo Ewald, Frank Leymann, Michael Pauly, J. Rutschlin, and David Schumm. Capturing cloud computing knowledge and experience in patterns. In *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, pages 726–733, 2012. 40, 41, 42, 45, 55, 63

[22] R.L. Grossman. The case for cloud computing. *it Professional*, 11(2):23–27, 2009. 25, 56

[23] Mohamed Hamdi. Security of cloud computing, storage, and networking. In *Collaboration Technologies and Systems (CTS), 2012 International Conference on*, pages 1–5, 2012. 5, 32, 37, 38, 45, 52, 57, 63, 64, 72

[24] A. Hammami, N. Simoni, and R. Salman. Ubiquity and QoS for cloud security. In *2012 41st International Conference on Parallel Processing Workshops (ICPPW)*, pages 277 – 278, September 2012. 38, 39, 41, 46, 57, 76

[25] J. Heiser and M. Nicolett. Assessing the security risks of cloud computing. *Gartner Report*, 2008. 27, 29, 52, 60

[26] Ghasem Heyrani-Nobari, Omar Boucelma, and St´ephane Bressan. Privacy and anonymization as a service: PASS. In Hiroyuki Kitagawa, Yoshiharu Ishikawa, Qing Li, and Chiemi Watanabe, editors, *Database Systems for Advanced Applications*, volume 5982, pages 392–395. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010. 9, 43, 44, 70

[27] Iliana Iankoulova and Maya Daneva. Cloud computing security requirements: A systematic review. In *Research Challenges in Information Science (RCIS), 2012 Sixth International Conference on*, pages 1–7, 2012. 3, 14,

[28] 16, 28, 37, 43, 44, 48, 58, 66, 73, 74

[29] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology. In *2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE)*, pages 1 –6, May 2012. 3, 25, 27, 29, 34, 41, 49, 54, 56, 57, 59, 63

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

[30] T. Jaeger and J. Schiffman. Outlook: Cloudy with a chance of security challenges and improvements. *Security & Privacy, IEEE*, 8(1):77–80, 2010. 9, 46
[31] W. Jansen and T. Grance. Guidelines on security and privacy in public cloud computing. *NIST Draft Special Publication*, pages 800–144, 2011. 26, 33, 43, 46, 49, 50, 52, 61, 63, 65, 69
[32] Shailza Kamal and Rajpreet Kaur. Cloud computing security issue: Survey. *AIP Conference Proceedings*, 1414(1):149–153, December 2011. 11, 25, 27, 29, 37, 52, 59, 60, 63, 69
[33] L.M. Kaufman. Data security in the world of cloud computing. *IEEE*
[34] *Security & Privacy*, pages 61–64, 2009. 11, 47
[35] Khaled M. Khan and Qutaibah Malluhi. Establishing trust in cloud computing. *IT professional*, 12(5):20–27, 2010. 46, 79
[36] Md Tanzim Khorshed, A. B. M. Ali, and Saleh A. Wasimi. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation Computer Systems*, 2012. 4, 13, 15, 16, 31, 33, 36, 40, 41, 47, 49, 51, 57, 58, 73
[37] G. Kulkarni, J. Gambhir, T. Patil, and A. Dongare. A security aspect in cloud computing. In *2012 IEEE 3rd International Conference on Software Engineering and Service Science (ICSESS)*, pages 547 –550, June 2012. 25, 33, 34, 37, 38, 47, 57, 63, 66
[38] Wenjun Luo and Guojing Bai. Multi-copy privacy-preserving verification for cloud computing. *International Journal of Advancements in Computing Technology*, 3(9):9–16, 2011. 28, 31, 75
[39] Xiaoqi Ma. Security concerns in cloud computing. In *Computational and Information Sciences (ICCIS), 2012 Fourth International Conference on*, pages 1069–1072, 2012. 11, 27, 28, 31, 33, 34, 39, 52, 66, 76
[40] Eystein Mathisen. Security challenges and solutions in cloud computing. In *Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on*, pages 208–212, 2011. 15, 25, 27, 38, 41, 44, 48, 49, 52, 54, 59, 64, 71, 79
[41] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology. In *2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE)*, pages 1 –6, May 2012. 3, 25, 27, 29, 34, 41, 49, 54, 56, 57, 59, 63
[42] Aryan Taheri Monfared and Martin Gilje Jaatun. Monitoring intrusions and security breaches in highly distributed cloud environments. In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on*, pages 772–777, 2011. 27, 33, 34, 37, 40, 46, 62
[43] L. Qiu, Y. Zhang, F. Wang, M. Kyung, and H.R. Mahajan. Trusted computer system evaluation criteria. In the National *Computer Security Center*, 1985. 29
[44] S. Ramgovind, Mariki M. Eloff, and E. Smith. The management of security in cloud computing. In *Information Security for South Africa (ISSA), 2010*, pages 1–7, 2010. 8, 10, 27, 29, 35, 38, 40, 42, 46, 51, 52, 54, 57, 59, 60, 63, 67, 69
[45] Laura Savu. Cloud computing: Deployment models, delivery models, risks and research challenges. In *Computer and Management (CAMAN), 2011 International Conference on*, pages 1–4, 2011. 25, 36, 38, 39, 42, 52
[46] N. K. Sehgal, Sohum Sohoni, Ying Xiong, David Fritz, Wira Mulia, and J. M. Acken. A cross section of the issues and research activities related to both information security and cloud computing. *IETE Technical Review*, 28(4):279, 2011. 11, 30, 33, 35, 38, 42, 44, 46, 57, 72

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07

[47] Avvari Sirisha and G. Geetha Kumari. API access control in cloud using the role based access control model. In *Trends in Information Sciences & Computing (TISC), 2010*, pages 135–137, 2010. 37, 73
[48] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K. Chaurasiya, and Rahul Gupta. An architecture based on a proactive model for security in cloud computing. In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, pages 661–666, 2011. 27, 29, 32, 33, 34, 37, 38, 40, 45, 49, 57, 58, 59, 60, 63, 73
[49] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, January 2011. 13, 25, 26, 27, 28, 29, 30, 31, 36, 38, 41, 47, 48, 49, 50, 53, 59, 65, 66, 67, 68, 69
[50] H. Takabi, J.B.D. Joshi, and G. Ahn. Security and privacy challenges in cloud computing environments. *Security & Privacy, IEEE*, 8(6):24–31, 2010. 8, 11, 45, 46, 50, 59, 64, 65, 66, 68, 70, 71
[51] J. Viega. Cloud computing and the common man. *Computer*, 42(8):106–8, 2009. Copyright 2009, The Institution of Engineering and Technology. 25, 26, 47
[52] S. William. *Network Security Essentials*. Pearson Education India, 2008. 38, 39
[53] Piers Wilson. Positive perspectives on cloud security. *Information Security Technical Report*, 2011. 25, 31, 45, 57
[54] Zhang Xin, Lai Song-qing, and Liu Nai-wen. Research on cloud computing data security models based on multi-dimension. In *Information Technology in Medicine and Education (ITME), 2012 International Symposium on*, volume 2, pages 897–900, 2012. 25, 32, 34, 37, 38, 46, 52, 60, 74
[55] Liang Yan, Chunming Rong, and Gansen Zhao. Strengthen cloud computing security with federal identity management using hierarchical IdentityBased cryptography. In *Proceedings of the 1st International Conference on Cloud Computing*, CloudCom '09, pages 167–177, Berlin, Heidelberg, 2009. Springer-Verlag. 24, 49
[56] Zhang Yandong and Zhang Yongsheng. Cloud computing and cloud security challenges. In *Information Technology in Medicine and Education (ITME), 2012 International Symposium on*, volume 2, pages 1084–1088, 2012. 29, 31, 34, 37, 41, 43, 49, 52, 59
[57] Huiming Yu, Nakia Powell, Dexter Stembridge, and Xiaohong Yuan. Cloud computing and security challenges. In *50th Annual Association for Computing Machinery Southeast Conference, ACM-SE'12, March 29, 2012 - March 31, 2012*, Proceedings of the Annual Southeast Conference, pages 298–302. Association for Computing Machinery, 2012. 25, 27, 36, 37, 38, 39, 40, 52, 73
[58] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable, and fine-grained data access control in cloud computing. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9, 2010. 3, 25, 30, 48, 77, 78
[59] Dimitrios Zissis and Dimitrios Lekkas. Addressing cloud computing security issues. *Future Generation Computer Systems*, (0), 2010. 28, 46, 53, 57, 69
[60] Stuart Charters and Barbara Kitchenham. Guidelines for performing systematic literature reviews in software engineering. (EBSE 2007-001), 2007.
[61] L. A Goodman. Snowball sampling. *The Annals of Mathematical Statistics*, 32(1):148–170, 1961. 19

Article DOI: 10.52589/AJSTE-BUIU5R07
DOI URL: https://doi.org/10.52589/AJSTE-BUIU5R07