ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

SECURITY AND PRIVACY ASPECTS OF CLOUD COMPUTING: A SMART CAMPUS CASE STUDY

[1]Mrs.G.Kousalya,[2]Mr.S.Nareshkumar Reddy,[3]Mrs.C.Indumathi,[4]Thippuluri Suma

[1,2,3]Assistant Professor,[4]Student

Department of CSE

Gouthami Institute Of Technology & Management For Women, Proddatur, Ysr Kadapa, A.P

ABSTRACT:

The trend of cloud computing is accelerating along with emerging technologies such as utility computing, grid computing, and distributed computing. Cloud computing is showing remarkable potential to provide flexible, costeffective, and powerful resources across the internet, and is a driving force in today's most prominent computing technologies. The cloud offers the means to remotely access and store data while virtual machines access data over a network resource. Furthermore, cloud computing plays a leading role in the fourth industrial revolution. Everyone uses the cloud daily life when accessing Dropbox, various Google services, and Microsoft Office 365. While there are many advantages in such an environment, security issues such as data privacy, data security, access control, cyber-attacks, and data availability, along with performance and reliability issues, exist. Efficient security and privacy measures should be implemented by cloud service providers to ensure the privacy, confidentiality, integrity, and availability of data services. However, cloud service providers have not been providing enough secure and reliable services to end users. Blockchain is a technology that is improving cloud computing. This revolutionary technology offers persuasive data integrity properties and is used to tackle security problems. This research presents a detailed analysis of privacy and security challenges in the cloud. We demonstrate the importance of security challenges in a case study in the context of smart campus security, which will encourage researchers to examine security issues in cloud computing in the future.

Keywords: Cloud computing; privacy concerns; security challenges; blockchain; data protection; data security

1 INTRODUCTION

The cloud provides a facility to store and access data from anywhere through an internet connection. With a cloud application, users can easily store their local data on a remote server [1]. According to Gartner [2], cloud computing is among the 10 most relevant technologies today. Individuals and organizations use it to share files and data. Cloud computing has gained the attention of the business community and academic researchers. Its architecture has reshaped information systems and is considered a part of the future driving technology. Cloud computing allows users to globally share information, services, and resources. The best examples are Google Apps, where anyone can access their data using applications via a web server. The storage of data in the cloud reduces the cost of hardware and improves the reliability of storage [3]. Cloud computing provides a shared pool of computing resources, such as storage devices, servers, networks, and services requiring minimal management effort. Meanwhile, it has many disadvantages. For instance, since it is made up of distributed networks, the cloud environment is vulnerable to the same

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

security threats as any network [4]. Its concept emerged from the grid and distributed computing domains used to host websites, mail servers, and web storage. Many cloud security attacks target a specific service or system. Hence, there is a need to classify such attacks according to the versatility of cloud services. Google announced in 2014 that data had been leaked through a URL associated with its Google Drive. Around 5 million accounts were hacked in 2015, leading to identity thefts, stolen blueprints, and loss of personal information.

The International Data Corporation (IDC) [5] surveyed 24 IT executives and found that the security risk of running apps was 74.1%. Various security checks must be deployed to maintain cloud computing security and prevent data breaches [6]. Providers such as Google, Amazon, and Microsoft teach their cloud customers how to implement security measures. A shortage of security engineers and specialists is the greatest security challenge to the cloud. Since computer-aided human activities depend on data, it is essential to trust be able to data. The critical nature of data has made it an attractive target of cyber-attacks aimed at compromising the basic confidentiality, integrity, and availability (CIA) properties that data require to be trusted [7,8]. Therefore, proper resolution of cloud security issues is important. Transferring data to the cloud tends to be tedious due to remote connectivity [9]. This paper identifies security and privacy concerns facing the cloud and explores their nature and possible solutions.

The remainder of this work is organized as follows. Section 2 presents related work. In Section 3, blockchain is discussed as it relates to the cloud, and Section 4 discusses security aspects. Some case studies are introduced in Section 5. Section 6 discusses our results. In Section 7, we provide our conclusions and propose directions for future work.

2 RELATED WORK

2.1 Cloud Computing

Since "cloud" refers to "the internet," the term "cloud computing" refers to the delivery of services via the internet. Cloud computing technology depends upon sharing resources with local servers or personal devices to control applications.

2.2 Cloud Service and Deployment Models

Amazon, Microsoft, Google, and Rackspace are the top cloud service providers [10]. Services presented by the cloud are categorized into three types. Data on the cloud can be accessed via cloud service models such as platform as a service (PaaS), infrastructure as a service (IaaS), and software as a service (SaaS) [11]. These models have different security environments and requirements.

2.2.1 Infrastructure as a Service

IaaS consists of an "on demand" internet connection and provides flexibility to increase or decrease the capacity of a server according to space. Examples include AWS EC2, Google Compute Engine (GCE), GoGrid, and 3tera. The cost factor of IaaS scales according to the client's utilization [12].

2.2.2 Platform as a Service

A PaaS client can rent hardware, operating systems, and network capacity to create cloud services limited only by the provider. The best examples are force.com and Microsoft Azure. Scalability, portability, flexibility, and user friendliness are some major advantages of PaaS. From

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

a security aspect, network- and host-based intrusions are challenges.

2.2.3 Software as a Service

In SaaS, clients use applications based on a cloud infrastructure. Applications can be accessed through web browsers, and clients rely on the service provider for proper security measures. The provider must ensure that users do not see each other's data. The four types of cloud deployment models are private, public, community cloud, and hybrid cloud. The private cloud infrastructure provides services to a client in their entirety and is preferred over public cloud due to its enhanced security. The public cloud operates for the general public through a cloud service provider while the community clouds work purely for an organization's consumer community. The community clouds are typically shared by groups of similar organizations. The hybrid cloud has characteristics of multiple models that are integrated by a standard technology that allows data portability.

2.3 Cloud Computing and Blockchain

Blockchain overcomes the key challenge of cost in cloud computing, enabling its decentralization to eliminate the risk of data violations. Although cloud computing tends to be cheaper than blockchain technology, it is quite expensive when used with a variety of objects. Blockchain enables the direct connection to massive GPU mining companies to gain their computing power. Moreover, blockchain storage accounts cannot easily be targeted or hacked, and thus it is difficult for a hacker to access large amounts of data through blockchain, whose data are stretched out as a chain and not together in one place [13].

2.4 Fundamental Cloud Computing Security Challenges

Privacy and security challenges depend on the nature of a business. For example, data are most crucial to the banking sector according to the privacy and integrity of its clients. The threats to and challenges of cloud computing security include those of access, trust, virtualization, software, and computation. The most prominent identified threat is to computation and access, which accounts for about 51% of all threats. Challenges to computation include cryptography malware, storage, and sanitization. Challenges regarding access are physical concerns and authentication. Confidentiality and data security are also prime security concerns, as data may be exploited by unauthorized users. Lack of control is also a large security issue relating to the cloud. Moreover, a cloud environment is vulnerable to cyberattacks, malicious insiders, cloud malware injection attacks, and XML signature element wrapping. An attacker creates a malicious application, adds it to the cloud layer, and treats this as a valid instance. Besides this, a virus or Trojan can be uploaded to the cloud [14]. Different security strategies can be implemented, such as standardization of APIs, public key infrastructure, and data distribution, to reduce the above risks. Access control, authentication, and authorization for the storage of data are essential to enhance security levels in cloud computing.

Here we highlight some recent cloud computing security incidents. To establish the reliability of the cloud, 11,000 papers were examined, covering the years 2008 to 2012 [15]. Only 129 of 172 cloud computing outages occurred for known

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

reasons. The most common threats were related to APIs as insecure interfaces comprising 29% of recorded threats, data loss and leakage at 25%, and hardware failure at 10%. Over 100 incidents were grouped in eight categories, and about 50 incidents were in none of these categories. Cloud computing is currently one of the most significant security challenges being addressed. A lack of security measures or their poor implementation can lead to great data-transmission risks. Rao and Selvamani emphasized that the strongest security solutions must be implemented to protect data from these security threats [16].

2.5 Blockchain Security in Cloud Computing

With the advent of next-generation financial technology, blockchain studies regarding the safe use of electronic cash have been conducted by communicating only between peers and without the involvement of third parties. The disclosure of user data in the cloud computing environment can compromise the user's personal information. However, privacy and anonymity studies are not enough. Blockchain can enhance security and ensure anonymity in a cloud computing environment [17].

2.6 Data Security Issues in Cloud Computing

Data security threats can be categorized as external or internal in the cloud environment. Internal threats occur mainly from insider attacks, and external threats from outside attacks as data is accessed by a third party. Attackers can obtain the personal information of a user. The cloud infrastructure should be scalable to ensure availability of data [18]. Six major security issues are listed below [19]:

Data integrity
Data privacy and confidentiality
Location of data
Availability of data Data storage, backup, and recovery
Data authentication.

3 BLOCKCHAIN

Several current studies apply blockchain technology to the cloud environment for data protection. Blockchain cryptographically links blocks, and the chain continues to grow. A block contains the cryptographic hash, timestamp, and transaction data of previous blocks. Modifications cannot be performed on the blockchain, and it effectively records transactions between stakeholders. Here we look at a study [20] on blockchain technology in data movement, data management, and cloud storage.

Kirkman Stephan [21] presented a cloud trust system that deals with blockchain. Normally, transparency is enhanced by lessening the problem due to trust on the third party. Ethereum and Hyperledger support smart contracts between various parties without the need for third parties. A cloud trust methodology with five degrees of recommendation was proposed using the belief and recommendation model. The trust of the threshold vendor was calculated, where trust relies on proof and experience. A smart contract was accessed through one public Ethereum address. A white list algorithm uses the "customer address" as the key in its hash table.

Yuzhe et al. [22] used the middleware system ChainFS to protect cloud storage. ChainFS is incorporated on Ethereum and S3FS with Fuse-based clients, and measures performance using Amazon S3; a low computational burden is observed in Chain FS. The ChainFS system consists of

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

a client and a cloud server managed, and is hosted by an unreliable blockchain. Fuse clients interact in two dimensions with remote parties. After verification, read operations are carried out using a Merkle proof, and a new root hash is used in place of the generated local state before it the operations are sent.

The Saranyu framework [23] includes the four services: identity management, authentication, authorization, and charging. Smart contracts run on a distributed ledger used to manage tenant and service accounts in a cloud computing center. Tab. 1 lists cloud security issues using blockchain.

Table 1: Survey on cloud security concerns

Reference Number	Solved problems	Blockchain techniques
[21]	Transparency issues related to TTPs	Ethereum and white list policy
[22]	Forgery attacks	SDFS and Ethereum
[23]	Tenant and service accounts	Smart contract and quorum
[24]	Data privacy	Demand response management, and public key infrastructure
[25]	Data traceability	DataProv, ProvChain and CoPS
[26]	Integrity verification	Two-layer blockchain network

4 Challenges and Privacy Aspects of Cloud Computing and Possible Solutions

The cloud computing environment faces various challenges and privacy concerns. Hence, effective security measures should be implemented. Tab. 2 identifies these challenges, their nature, and possible solutions.

Table 2: Challenges and privacy aspects of cloud computing, and their possible solutions

Cloud security challenges/concerns	Nature of problem	suggested solutions
Data Security and confidentiality issues [27]	Data confidentiality	Hashing and encryption
Browser security [27]	Web Service Security	SSL/TSL for client authentication
Data availability and reliability issues [27]	Uncertainty in service of reliability	Authorization and authentication
Data loss or leakage prevention	Unauthorized access to infrastructural components	Fragmentation redundancy and scattering techniques [28]
Access control [29]	Illegitimate access	Enforcement of access policies
Eavesdropping and confidentiality [30]	Eavesdropping and alteration	Proper integration and confidentiality mechanism
Data Authentication [31]	Unauthorized access	Application of one-way hash function [32]
Data privacy and integrity	Unauthorized access	Native and integrity mechanisms
DoS attack	Malicious attacks	Cryptographic techniques
Malicious insiders	Loss of data integrity and confidentiality	Standard cryptographic algorithms
Spoofing, phishing [33]	Data forgery	IPS and IDS
Distributed denial of service (DDoS) [34]	DDoS	Fuzzy logic-based mechanisms

5 CASE STUDY

We conducted a survey related to security aspects of cloud computing in a smart campus domain, and had 100 respondents. This survey allowed us to identify the cloud security and privacy concerns of people who are either directly or indirectly involved in a smart campus community.

Table 3 shows that the 100 respondents consisted of 33% females and 67% males. They belonged to different job sectors, mostly in the technical and computer science domains, with some knowledge of cloud computing and its associated storage, services, security, and privacy aspects. Our survey instrument considered the smart campus domain, in which hundreds of smart devices share data with people, machines, and each other. We solicited respondents' opinions on the security and privacy aspects of cloud servers when dealing with smart campus data.

Table 3: Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	33	33.0	33.0	33.0
	Male	67	67.0	67.0	100.0
	Total	100	100.0	100.0	

Tab.5 We asked if people believed their smart campus data could not be stolen if stored on a cloud server. Tab. 4 indicates that 50% of respondents were not confident enough to answer this question via "Yes" or "No". This might be due to a misunderstanding about cloud data storage and security policies. Furthermore, respondents were not sure how cloud servers manage data storage and who can access the data.

Table 4: Do you think that no one can ever steal your smart campus data?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	46	46.0	46.0	46.0
	Disagree	46	46.0	46.0	92.0
	Neutral	8	8.0	8.0	100.0
	Total	100	100.0	100.0	

IJFANS International Journal of Food And Nutritional Sciences
Official Publication of International Association of Food and Nutrition Scientists

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

presents opinions of respondents on firewalls and other protective measures of cloud computers. We can observe that 87% believed that by using these protective measures, cloud managers can better incorporate the security aspects of data. This positive response indicates that respondents are happy to employ cloud services provided by the cloud stakeholders and can adopt necessary precautionary measures to safeguard precious smart campus data.

The data in Tab. 6 indicate that 79% of respondents strongly believed that cloud-based storage of smart campus data is under security threat. Most people assume that cloud services are more vulnerable to security threats if cloud managers do not ensure security and privacy. Illegitimate access to data is always a security challenge. The other 21% of respondents also described the cloud as vulnerable to security issues. Cloud managers and stakeholders can address these concerns through strict security measures.

Tab.7 summarizes responses to the question of whether cloud storage of sensitive smart campus data is under greater security risk than distributed data storage. This is similar to the data presented in Tab. 6. Most respondents believed cloud storage was vulnerable to security threats; 92% thought distributed data storage was safer.

Table 5: The firewall and other protective measures of cloud computers can protect the smart campus data in most cases?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	8	8.0	8.0	8.0
	Disagree	13	13.0	13.0	21.0
	Strongly Agree	79	79.0	79.0	100.0
	Total	100	100.0	100.0	

Table 6: The cloud-based smart campus data is vulnerable to security threats?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	21	21.0	21.0	21.0
	Strongly Agree	79	79.0	79.0	100.0
	Total	100	100.0	100.0	

Table 7: The cloud storage of sensitive smart campus data is under security risk compared to distributed data storage?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	92	92.0	92.0	92.0
	Disagree	8	8.0	8.0	100.0
	Total	100	100.0	100.0	

We asked if there is usually no chance for thieves of smart campus data to be caught. Tab. 8 shows that 92% of respondents agreed that this is usually the case.

Table 8: If smart campus data is illegitimately taken, then there will suitable ways to catch culprits?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	92	92.0	92.0	92.0
	Neutral	8	8.0	8.0	100.0
	Total	100	100.0	100.0	

Tab.9 shows that 92% of respondents thought that cloud storage of smart campus data meets privacy demands.

Table 9: Do you think smart campus data's cloud storage will maintain that data privacy?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	92	92.0	92.0	92.0
	Disagree	8	8.0	8.0	100.0
	Total	100	100.0	100.0	

Fig.1 presents the level of trust of managers and common users in cloud storage in the scenario of a smart campus study. Some 56% of respondents believed that cloud managers have concerns related to security aspects of smart campus data being handled by cloud servers, and 62% agreed to report the loss of smart campus data. Some 66% thought that cloud servers have reliable recovery plans. On a broad level, we can understand that a cloud management team is more confident than users regarding the security of cloud data storage. The cloud users have a similar opinion but with certain concerns. Still, the users realize that the cloud is a significant

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

option to store their valuable data despite the security challenges and issues.

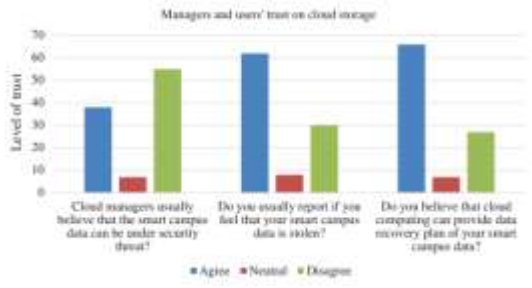

Figure 1: Managers and users' level of trust in cloud storage

Fig.2 addresses the security aspects of cloud storage. We can see that 76% of stakeholders were willing to keep their data on the cloud, and 46% believed that cloud storage comes with security issues. Many participants provided a neutral response, which indicates uncertainty. Furthermore, 76% of respondents believed that cloud storage for a smart campus is important despite security challenges. Here, we observe that people mostly trust cloud servers for smart campus data management irrespective of security issues.

Fig. 3 shows the scalability concerns for cloud storage. We can see that 78% of stakeholders believed that cloud managers and smart campus stakeholders should coordinate on the policies for smart campus data management on cloud servers so as to maximize data protection. Similarly, 56% of people believed that cloud storage provides scalable solutions. A small number of participants gave a neutral response, which indicates uncertainty related to the scalability of the cloud. Moreover, 78% of respondents believed that vertical scalability is more appealing than horizontal scalability. A small number of respondents did not provide feedback, while another small number of respondents thought horizontal scalability better than vertical scalability.

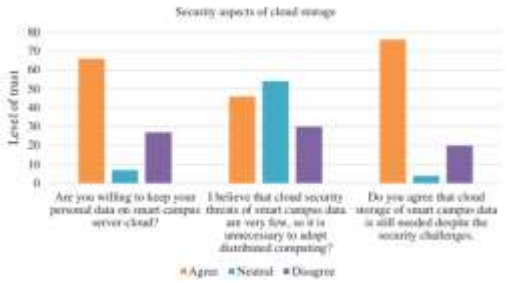

Figure 2: Security aspects of cloud storage

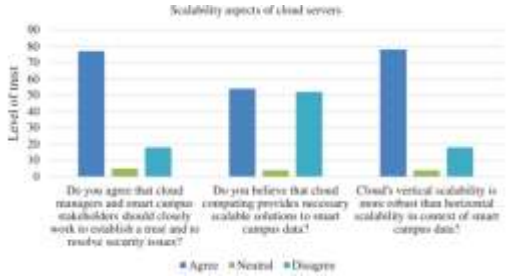

Figure 3: Scalability aspects of cloud storage

6 DISCUSSION

Cloud computing is an evolving, internet-based technology that tends to dominate in computer science and information technology applications that involve large-scale network computing. Cloud computing is a shared pool of resources that is gaining popularity because of its affordability, performance, and availability. Cloud computing faces challenges including data privacy, intellectual property rights, data security, and authenticated access. We studied its security and privacy through a case study in a smart campus scenario.

We seek to highlight the major security vulnerabilities in cloud computing since it has become the most commonly used method of virtualization in large and modern data centers and cloud infrastructures [35]. The major threats and open security issues are a breach of data, IP spoofing, ARP spoofing, DNS poisoning, injection with SQL, injection with OS, LDAP injection, orchestration of

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

the cloud, and zombies or DDoS [36]. Jain and Jaiswal emphasized cloud security parameters: cloud network, database, operating system, virtualization, resource allocation, transaction management, load balancing, memory management, and concurrency control. Cloud security can be classified as data concerns, privacy risks, and problems with compromised apps and confidentiality. A report on cloud security problems and challenges identified vulnerabilities dependent on browsers, such as phishing, SSL certificates, spoofing, and browser cache attacks. Data integrity is impacted by inadequate encryption, lack of audit control, authentication, and authorization. The authors in varsha et al. [37] examined security problems in cloud computing, and identified the top seven security problems. The Cloud Protection Alliance (CSA) discovered security problems, and multi-tenancy was the main security concern discussed.

7 CONCLUSIONS

We categorized the security and privacy aspects of the cloud, concentrating on a case study set in a smart campus scenario. We discussed security issues such as data privacy, access control, and data availability. The lack of security measures and ease of access in the cloud can result in the compromise of data without the victim's knowledge. Security issues in cloud applications must be recognized, and safety measures taken in communication networks. Hence, it is emphasized to deploy the efficient security and privacy measures to ensure data integrity, privacy, and reliability. However, cloud service providers are not providing enough security to satisfy users. Additionally, blockchain improves security problems in cloud computing. We highlight cloud security concerns/challenges and their behavior/nature with suggested solutions that will benefit other researchers.

Acknowledgement:

The authors would like to thank for the support from Taif University Researchers Supporting Project number (TURSP-2020/10), Taif University, Taif, Saudi Arabia.

Funding Statement: We are thankful to the College of Sciences and Arts in Rass, Qassim University, Buraydah 51452, Saudi Arabia, for the funding support.

Conflicts of Interest: Authors declare that they have no conflicts of interest in this research.

REFERENCES

[1] N. Santoso, A. Kusyanti, H. P. A. Catherina and Y. A. L. Sari, "Trust and security concerns of cloud storage: An indonesian technology acceptance," International Journal of Advanced Computer Science and Applications, vol. 9, no. 6, pp. 453–458, 2018.

[2] S. Giri and S. Shakya, "Cloud computing and data security challenges: A nepal case," International Journal of Engineering Trends and Technology, vol. 67, no. 3, pp. 146–150, 2019.

[3] N. Hemalatha, A. Jenis, A. C. Donald and L. Arockiam, "A comparative analysis of encryption techniques and data security issues in cloud computing," International Journal of Computer Applications, vol. 96, no. 16, pp. 1–6, 2014.

[4] M. Ahmed and A. T. Litchfield, "Taxonomy for identification of security issues in cloud computing environments," Journal of Computer Information Systems, vol. 58, no. 1, pp. 79–88, 2018.

[5] M. Durairaj and A. Manimaran, "A study on security issues in cloud based e-

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 11, Iss 11, 2022

learning," Indian Journal of Science and Technology, vol. 8, no. 8, pp. 757–765, 2015.

[6] P. R. Kumar, P. H. Raj and P. Jelciana, "Exploring data security issues and solutions in cloud computing," Procedia Computer Science, vol. 125, pp. 691–697, 2018.

[7] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri et al., "Blockchain-based database to ensure data integrity in cloud computing environments," in Proc. Int. Conf. on Mainstreaming Block Chain Implementation (ICOMBI), pp. 1–4, 2020.

[8] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, vol. 79, pp. 88–115, 2017.

[9] I. Ahmed, "A brief review: Security issues in cloud computing and their solutions," Telkomnika, vol. 17, no. 6, pp. 2812–2817, 2019.

[10] Y. Sun, J. Zhang, Y. Xiong and G. Zhu, "Data security and privacy in cloud computing," International Journal of Distributed Sensor Networks, vol. 10, no. 7, pp. 190903, 2014.

[11] M. J. Kavis, Architecting the cloud: Design decisions for cloud computing service models (SaaS, PaaS, and IaaS), John Wiley & Sons, 2014.

[12] R. Bhadauria and S. Sanyal, "Survey on security issues in cloud computing and associated mitigation techniques," preprint arXiv: 1204. 0764, 2012.

[13] S. Pavithra, S. Ramya and S. Prathibha, "A survey on cloud security issues and blockchain," in Proc. 3rd Int. Conf. on Computing and Communications Technologies (ICCCT), pp. 136–140, 2019.

[14] D. Jamil and H. Zaki, "Security issues in cloud computing and countermeasures," International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 4, pp. 2672–2676, 2011.

[15] M. S. Almutairi, "Cloud computing: Securing without losing control," Journal of Advances in Mathematics and Computer Science, vol. 31, no. 2, pp. 1–9, 2019.

[16] R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," Procedia Computer Science, vol. 48, pp. 204–209, 2015.

[17] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," Symmetry, vol. 9, no. 8, pp. 164, 2017.

[18] M. A. Razzaq, J. A. Mahar, M. A. Qureshi and Z. U. Abidin, "Smart campus system using internet of things: Simulation and assessment of vertical scalability," Indian Journal of Science and Technology, vol. 13, no. 28, pp. 2902–2910, 2020.

[19] S. A. Hussain, M. Fatima, A. Saeed, I. Raza and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," Applied Computing and Informatics, vol. 13, no. 1, pp. 57–65, 2017.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE international congress on big data (BigData congress), pp. 557– 564, 2017.