IJARASEM

ISSN: 2395-7852

International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 11, Issue 6, November - December 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.583

☎ +91 9940572462 ☎ +91 9940572462 ✉ ijarasem@gmail.com @ www.ijarasem.com

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 7.583 | Bimonthly, Peer Reviewed & Referred Journal|

| Volume 11, Issue 6, November-December 2024 |

An Analysis of a Smart Campus's Security and Privacy Concerns with Cloud Computing

Sharath Gowda N R, Varun Gowda H R, Kotersh Naik D, Suhas K C, Mahesh N

U.G. Student, Department of Computer Engineering, CIT College, Tumkur, Karnataka, India

U.G. Student, Department of Computer Engineering, CIT College, Tumkur, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, CIT College, Tumkur, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, CIT College, Tumkur, Karnataka, India

Assistant Professor, Department of Computer Science and Engineering, CIT College, Tumkur, Karnataka, India

ABSTRACT: Alongside new innovations such as grid computing, utility computing, and distributed computing, the cloud computing trend is growing faster. Cloud computing is a major factor in today's most well-known computing technology and is demonstrating amazing promise to deliver flexible, affordable, and formidable resources over the internet. As virtual machines retrieve information via a network resource, the cloud provides the ability to access and store data remotely. Moreover, the fourth industrial revolution is largely driven by cloud computing. Everybody uses the cloud on a regular basis to access Microsoft Office 365, Dropbox, and other Google services. While there are numerous advantages to such an environment, there are security issues as well, including performance and reliability issues, access control, data security, and data privacy, cyberattacks, and data availability. Cloud service providers should use effective privacy and security measures to ensure the privacy, confidentiality, integrity, and availability of data services. However, cloud service providers' services have not been sufficiently safe and dependable for end users. Blockchain is one technology that is improving cloud computing. This innovative method tackles security concerns while offering strong data integrity features. This study looks closely at the security and privacy concerns with the cloud. Through a case study, we highlight the significance of security challenges in the context of smart campus security, which will motivate future academics to look into security concerns in cloud computing.

KEYWORDS: Blockchain, cloud computing, privacy issues, security difficulties, data security, and data protection

I. OVERVIEW

The cloud offers the ability to store and retrieve data from any location with an internet connection. With the help of a cloud application, users can conveniently save their local data on a remote server [1]. According to Gartner, cloud computing is one of the top ten most important technologies [2]. Both consumers and businesses utilize it to share files and data. Cloud computing is gaining attention from both academic researchers and the business community. Its architecture has transformed information systems and is seen as a part of the technology that will propel the future. Users may share resources, services, and information globally thanks to cloud computing. One of the better examples is Google Apps, which allows anyone to use programs through a web server to access their data. Cloud-based data storage lowers hardware costs and increases storage dependability [3]. A shared pool of computer resources, including servers, storage devices, networks, and services, is made available by cloud computing with little administration work. In the meanwhile, it has a lot of drawbacks. For example, the cloud environment is susceptible to the same security risks as any network because it is composed of dispersed networks [4]. Its concept originated in the distributed computing and grid domains that host mail servers, websites, and online storage. A specific system or service is the target of several cloud security attacks. As a result, these attacks must be categorized according to how flexible cloud services are. Google revealed in 2014 that a URL linked to Google Drive had hacked data. Approximately 5 million accounts were compromised in 2015, leading to personal data loss, identity fraud, and blueprint theft.

II. RELATED WORKS

2.1 Cloud-Based Computing

Given that "cloud" means "the internet," "cloud computing" describes the provision of services through the internet. In order to manage apps, cloud computing technology relies on resource sharing with nearby servers or personal devices.

2.2 Models for Cloud Services and Deployment

Amazon, Microsoft, Google, and Rackspace are among the leading providers of cloud services [5]. The services that the cloud provides fall into three categories. Users can access data on the cloud through cloud service models such as software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS) [6]. These goods have different security contexts and requirements.

2.2.1 Service-Based Infrastructure

IaaS includes a "on demand" internet connection and allows a server's capacity to be scaled according to available space. Examples include GoGrid, Google Compute Engine (GCE), and AWS EC2. The cost of IaaS fluctuates according to the customer's usage [7].

2.2.2 Platform as a Service

A PaaS customer can rent network bandwidth, operating systems, and hardware to build cloud services that are only limited by the provider; the best examples are Microsoft Azure and force.com. PaaS offers a number of important advantages, such as scalability, mobility, flexibility, and user-friendliness. Security challenges are caused by host-based and network-based intrusions.

2.2.3 Software as a Service

SaaS customers use apps that are developed on top of cloud infrastructure. Applications can be accessed using web browsers, and users rely on the service provider to put in place the necessary security measures. The supplier is in charge of ensuring that users are unable to see one another's data. There are four types of cloud deployment models: private, public, communal, and hybrid. Private cloud architecture gives services to a client in its entirety and is preferred over public cloud due to its enhanced security. Public clouds operate for the general public through cloud service providers, whereas community clouds cater only to an organization's clientele. Community clouds are typically shared by groups of linked organizations. The hybrid cloud incorporates elements from several services.

2.3 Blockchain and Cloud Computing

The main economic problem with cloud computing is resolved by blockchain, which also enables decentralization to lower the risk of data breaches. Even though cloud computing is typically less expensive than blockchain technology, it can still be very expensive when applied to a variety of products. Blockchain enables direct access to the processing capacity of major GPU mining companies. It is also difficult for a hacker to access large amounts of data via blockchain, which are distributed as a chain rather than collected in one place, because blockchain storage accounts are hard to target or hack.

2.4 Fundamental Security Concerns with Cloud Computing

The security and privacy challenges are determined by the sort of business. The banking sector, for example, depends significantly on data to safeguard the privacy and integrity of its clients. Among the threats and challenges facing cloud computing security include access, trust, virtualization, software, and computation. About 51% of all attacks are related to computation and access, making this the most significant hazard that has been detected. Storage, sanitization, and cryptography viruses are computational challenges. Physical issues and authentication present access challenges. Since data might be misused by unauthorized users, confidentiality and data security are also of the utmost importance. Another major cloud security concern is an absence of authority. Here, we list a few recent cloud computing security incidents. The reliability of the cloud was assessed by reviewing 11,000 papers from 2008 to 2012 [15]. Just 129 of the 172 cloud computing outages had known reasons. The most often reported threats were APIs (29%), followed by unsecured interfaces (29%), hardware failure (10%), and data loss and leakage (25%). About 50 occurrences fell into none of the eight classifications that more than 100 incidents were divided. One of the biggest security issues being addressed right now is cloud computing. High data-transmission hazards can result from inadequate security measures or from their improper application. Rao and Selvamani stressed that the most effective security measures

2.5 Utilizing Blockchain regarding the security of cloud computing

Since the launch of next-generation financial technology, blockchain research on the secure usage of electronic currency has been executed. Solely among peers and without the assistance of outside parties. User privacy may be jeopardized if user data is disclosed within a cloud computing setting. Studies on anonymity and privacy, however, are insufficient. In a cloud computing setting, blockchain can improve security and guarantee anonymity [8].

2.6 Cloud Computing Data Security Issues

In a cloud setup, there are two kinds of data security threats: internal and external. When an outsider party accesses data, external hazards arise from outside attacks, while internal threats are generally brought on by insiders attacks. Attackers can obtain a user's private information data.

III. BLOCKCHAIN

Blockchain technology is employed in a number of recent studies to protect data in cloud environments. Blocks are cryptographically connected by blockchain, and the chain keeps expanding. The timestamp, transaction information, and cryptographic hash of earlier blocks are all contained in a block. The blockchain efficiently records transactions between stakeholders and prevents modifications. Here, we examine a study [9] on the use of blockchain technology in cloud storage, data management, and data transfer.

A blockchain-based cloud trust mechanism was introduced by Kirkman Stephan [9]. Usually, reducing the issue because of the third party's confidence improves transparency. Smart contracts between many parties are supported by Ethereum and Hyperledger without the involvement of third parties. The belief and recommendation model was used to offer a cloud trust approach with five degrees of endorsement. Since trust is based on evidence and experience, the threshold vendor's trust was calculated. A single Ethereum public address was used to access a smart contract. The "customer address" is the key in the hash table of a white list algorithm.

In order to protect cloud storage, Yuzhe et al. [10] used the middleware system ChainFS, which is based on Ethereum and S3FS with Fuse-based clients and measures performance using Amazon S3. The ChainFS system is composed of a client and a cloud server managed by an unreliable blockchain, and Fuse clients communicate with remote parties in two dimensions. Following verification, Read operations are performed. Using Merkle proof, and before the operations are sent, a new root hash is employed instead of the generated local state.

IV. CASE STUDY

We polled 100 people about the security features of cloud computing within the context of smart campuses. We were able to ascertain the privacy and cloud security concerns of individuals who are directly or indirectly participating in a smart campus community thanks to this poll. According to Tab. 3, of the 100 responders, 67% were men and 33% were women. They worked in numerous fields, primarily in technology and computer science, and had some familiarity with cloud computing and the storage, services, security, and privacy features that go along with it. The smart campus domain, where hundreds of smart gadgets exchange data with people, machines, and one another, was considered into consideration by our survey tool. We inquired about the opinions of the respondents about the privacy and security features.

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 lacked sufficient confidence to answer this question via “Yes” or “No”. This might be due to a misunderstanding about cloud data storage and security policies. Furthermore, respondents lacked clarity regarding how cloud servers manage data storage and who can access the data. 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 affirmative reaction suggests that respondents are happy to employ cloud services provided through 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 think 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 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 option to store their valuable data despite the security challenges and issues.

The degree of trust that managers and regular users have in cloud storage within the framework of a smart campus research is displayed in Figure 1. About 62% of respondents agreed to report the loss of smart campus data, and 56% of respondents said that cloud administrators were worried about the security elements of the data handled by cloud servers. 66% of respondents said that cloud servers had dependable backup strategies. Broadly speaking, we can comprehend that a cloud management team has greater faith in the security of cloud data storage than do users. Despite their reservations, cloud consumers have a similar viewpoint. Despite the security problems and limitations, users still recognize that the cloud is a crucial choice for storing their valuable data.

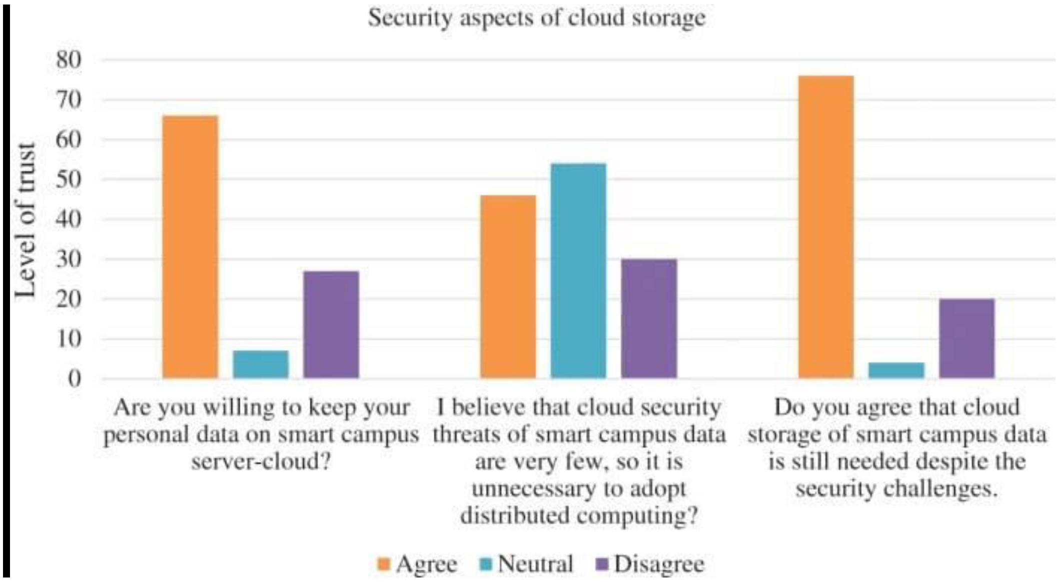

Figure 1: The degree of trust that managers and users have in cloud storage

Figure 2 discusses cloud storage's security features. As we can see, 46% of stakeholders thought that cloud storage had security risks, whereas 76% of stakeholders were happy to keep their data on the cloud. Uncertainty is indicated by the neutral responses given by several individuals. In addition, despite security concerns, 76% of respondents thought cloud storage was crucial for a smart campus. Regardless of security concerns, we may observe that the majority of people have faith in cloud servers for managing data on smart campuses.

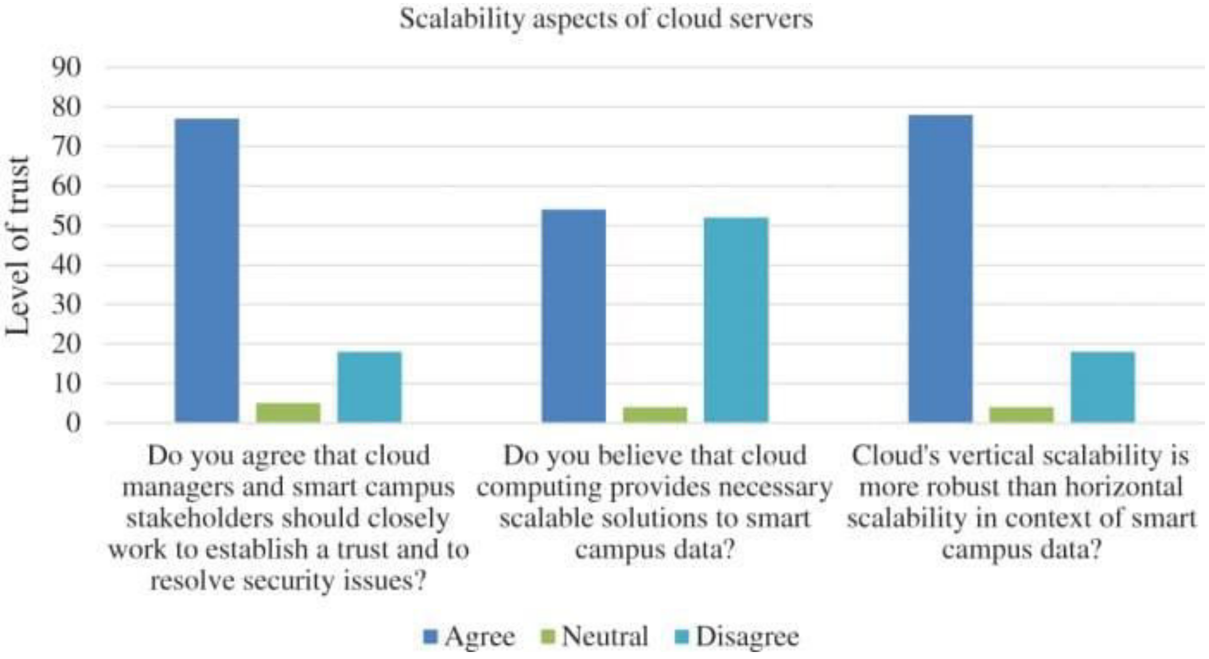

Figure 2: Cloud storage security features

Figure 3 demonstrates the issues with cloud storage scalability. As we can see, 78% of stakeholders thought that in order to optimize data protection, cloud managers and smart campus stakeholders should work together on the policies for managing data on cloud servers. Likewise, 56% of respondents said that scalable solutions were offered by cloud storage. A small percentage of respondents provided a neutral response, indicating a lack of confidence in the cloud's scalability. Furthermore, according to 78% of respondents, vertical scalability is preferable to horizontal scalability. Only a small percentage of respondents gave no input, and even fewer believed that horizontal scalability was superior to vertical scalability.

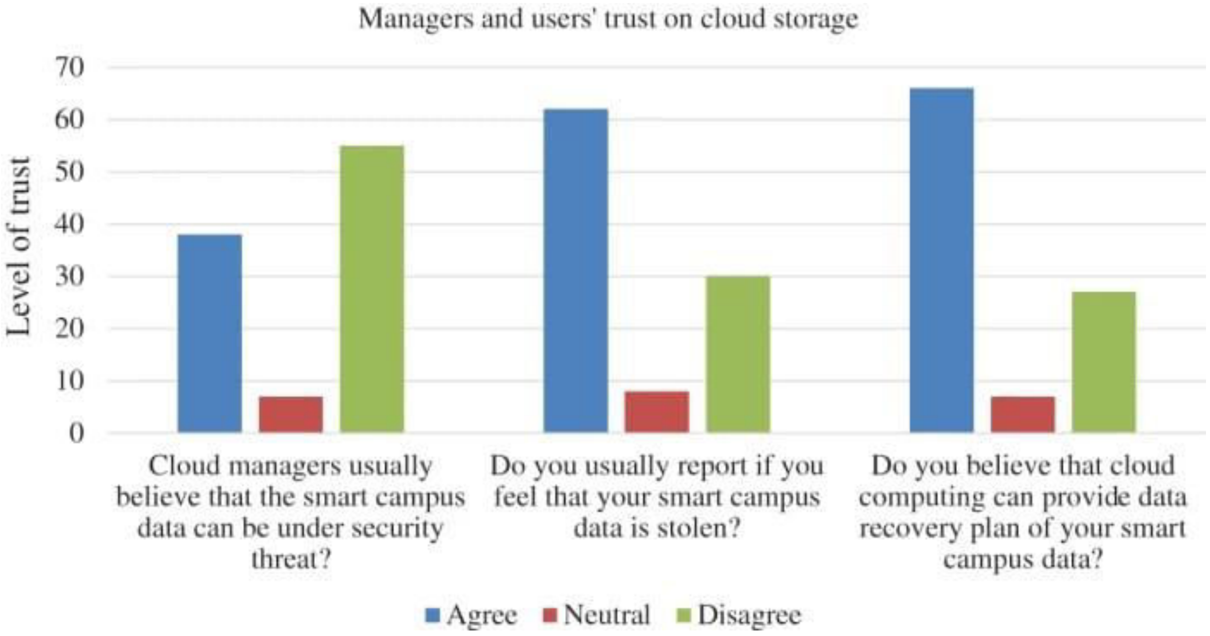

Figure 3: Cloud storage's scalability features

V. DISCUSSION

The use of 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 rights to intellectual property and data privacy, 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 [11]. The major threats and open security issues are a breach of data, ARP spoofing, DNS poisoning, IP spoofing, injection with SQL, injection with OS, LDAP injection, orchestration of the cloud, and zombies or DDoS [12]. Jain and Jaiswal emphasized cloud security parameters: cloud operating system, database, network, 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. [13] 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 primary security issue discussed.

VI. CONCLUSIONS

With an emphasis on a case study located within an intelligent campus scenario, we characterized the cloud's security and privacy features. We talked about security concerns such data availability, access management, and privacy. Without the victim's knowledge, data might be compromised due to the cloud's ease of use and absence of security controls. It is necessary to identify dangers to cloud application security and implement precautions in communication networks. In order to guarantee data integrity, privacy, and dependability, it is crucial to put in place efficient privacy and security measures. But users are dissatisfied with the level of security offered by cloud service providers. Blockchain also helps with protection of cloud computing issues.

In order to help other academics, we highlight problems and difficulties with cloud security along with their nature and behavior and offer potential solutions.

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-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.

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com