Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2019, 6(11):112-118

Research Article ISSN: 2394 - 658X

A Comprehensive Analysis of Next-Generation Approaches to Securing Hybrid Cloud Environments

Sri Kanth Mandru

mandrusrikanth9@gmail.com

ABSTRACT

This article aims to evaluate and explain the most effective methods for protecting hybrid cloud environments, with a particular focus on integrating various technologies of the future generation. One of the concepts being considered addresses the conceptual issues associated with hybrid cloud solutions. These issues include data security, privacy, and integrity. Consequently, this article offers a security framework based on technologies such as Blockchain, edge computing, software-defined networking, and RBAC. This research evaluates the effectiveness, applicability, and issues associated with these approaches and provides information about how to implement them in modern information technology systems.

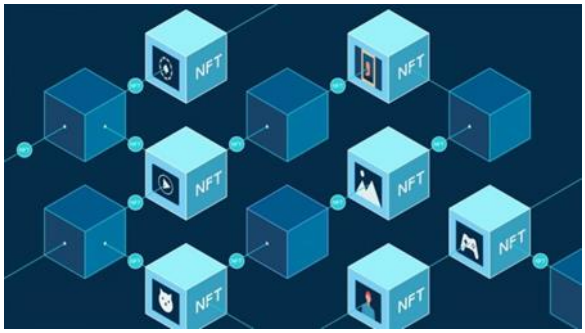
Keywords: Cloud Computing, Edge Computing, Security and Privacy, Blockchain, Edge Computing, Software Networking (SDN), Role Base Access Control (RBAC), Data Privacy, and Data Authenticity

---

INTRODUCTION

Cloud computing is one of the most significant IT trends because it is flexible, scalable, and inexpensive. This allows organizations to access gross computational resources on call, enhancing creativity and efficiency. However, with solutions like a hybrid cloud that combines the characteristics of both private and public clouds, the security issue is awakened [1]. Several risks arise from integrating these systems and data exchange between these systems; thus, effectively implementing serious security measures is necessary in such contexts.

There is a specific preposterous situation in those instances when organizations face multiple levels of hybrid cloud environments where security is much riskier [2]. Security methods must be facilitated to adequately address confidentiality, integrity, and data access to blend private and public clouds. About these issues, new solutions associated with hybrid cloud security can be designed.



Hence, this paper provides a framework for Blockchain, edge computing, SDN, and RBAC to solve fourth-generation hybrid cloud security challenges. Based on the concept of decentralization and the system's inherent immutability, such as the Blockchain, it is possible to enhance the data's reliability and confidentiality. Blockchain excludes data theft scenarios and offers a secure means of cloud data flow monitoring, as all the transactions are recorded irreversibly.

Latency and security are achieved through edge computing of data processing close to the point of data creation. It decreases cases where data is intercepted, especially by hackers, and provides timely decisions since data is processed locally in edge computing. Security threats can be tackled in real time with the help of software-defined networking (SDN) of networks' configurations, according to a study by Allon [3]. This functionality is crucial for providing data from the point of view of maintaining its integrity and readiness in unplanned hybrid cloud connectivity with possibly unpredictable network traffic.

RBAC stands for role-based access control, which limits or grants a user access to a specific resource based on the role assumed by that user, enhancing security [4]. It reduces internal threats due to limitation of access while at the same time, granting the user a proper amount of privileges.

The following is the proposed architecture incorporating these new technologies to deal with hybrid cloud security challenges: This method increases the aspects of hybrid cloud which makes them ideal to contemporary IT structures in terms of security, performance and flexibility. However, to propose a suitable hybrid cloud structure, this study only assesses these technologies' advantages, usefulness, and limitations.

PROBLEM STATEMENT

Hybrid cloud settings are made by layering the public cloud, which is widely recognized for its flexibility, over the private cloud, which is well known for its structure, it is essential to realize that hybrid cloud environments are bound to be complex. This is because hybrid cloud environments are formed by layering the public cloud. This complexity gives rise to several security concerns, including:

A. Data Confidentiality and Privacy

Another unique challenge that needs to be addressed when sharing data between multiple cloud structures is data security and privacy as the data moves from one environment to another. Following the study conducted by Rathore et al. in 2017, the transfer of information across public clouds and the architectures that combine public and private clouds is much more dangerous than it may seem because it is easy to seize the data being transferred [4]. Even though conventional security technologies are beneficial to some extent, they are overused more than needed for the superimposed cloud, which is usually fluid and dispersed [5]. Trusted data storage and data protection in such a context requires highly sophisticated encryption algorithms and secure key management frameworks that are scalable to the inherently fluid nature of a hybrid cloud environment.

B. Data Integrity

The repercussions of data changes must be easily identified and mitigated over physical and virtualized hybrid cloud structures. Hybrid cloud computing models are also divided into different parts, making it somewhat challenging to synchronize typical security policies between cloud components and the surroundings. Thus, it becomes vulnerable to experiencing data manipulation and data corruption more often. In a hybrid cloud context, data authenticity is a significant concern. Hence, to achieve data consistency between different servers, there is a need for equally consistent fine-grained observing, scanning, and checkout for any inconsistent changes. Therefore, using such measures presupposes the availability of sufficient knowledge of the characteristics of the interactions occurring in the functioning of the hybrid cloud.

C. Access Control

In reality, controlling who has access to what resources within the systems is feasible while providing the highest level of comfort and security. This is apparent in the instance being considered. According to Alkadi et al. who carried out the research in 2019, only the designated individuals should have access to the appropriate data and tools [6]. Even though it is complicated and limited to certain software tools and technologies, discussing access control in a hybrid cloud environment may sound easy. The presence of these settings suggests that the techniques used for access control are not fixed and can adjust to the environment. They must consider the authorization of services in a dynamic environment and the security defined for that kind of topology. The notion of the general security plan is adhered to in this manner, allowing for suitable control over such access [6]. Dynamic access control mechanisms could assist in preventing such dangers by adjusting to the existing circumstances while also being dependable in providing adequate security control and operation.

SOLUTIONS

A. Blockchain-Enabled Security Framework

As for Blockchain, this structure's decentralization and security properties guarantee that all transactions are actual and that the application's core structure will be secure. Thus, the integration of edge computing along with software-defined networking and Blockchain enriches the concept of a hybrid cloud system with the proper security it deserves [3]. Due to these challenges, a Blockchain-enabled security framework efficiently underpins the Building Information Model data confidentiality, integrity, and access control. This framework takes advantage of Blockchain's key characteristics: the decentralization and the inability to change data since such means can easily be noticed, and power is not concentrated in one point.

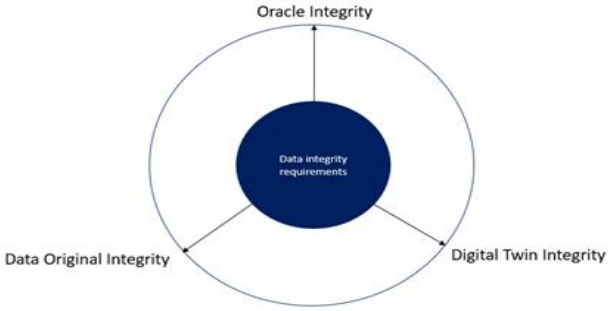
Edge computing supplements this approach by processing data in real-time, where it is produced within a network [7]. This proximity minimizes latency and optimizes the system requiring a fast response, especially in dynamic and

context-sensitive security systems. Moreover, SDN has dynamic network management that can quickly change according to the new requirements and overall conditions.

Thus, the proposed security framework could confront several issues connected with using hybrid clouds by integrating the technologies mentioned above above-mentioned. That way, data access frequency is constantly checked and adapted according to the current state of affairs, which must improve the protection and performance simultaneously. This approach enhances the security of data and the system's reliability and performance in the hybrid cloud, making it a one-stop solution.

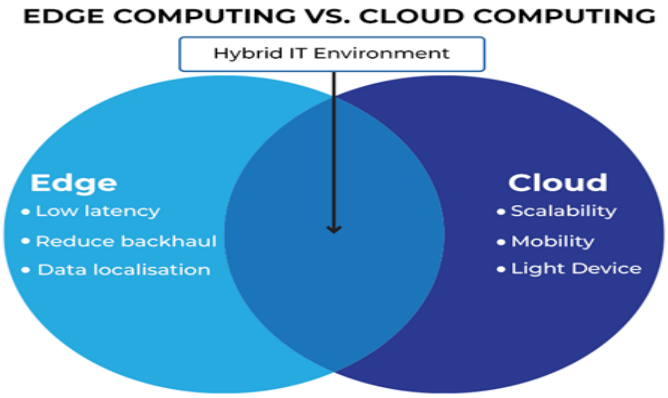
B. Blockchain for Data Integrity and Confidentiality

The tamper-proof feature of the blockchain technique makes it possible for data to be stored securely and without being altered on the Blockchain. According to research by Wang and Kogan in 2018, a fixed ledger system that is both transparent and shared makes it extremely difficult for any participant to perpetrate fraud [8]. With this system, every value or information movement occurs [9]. Because data migration will frequently occur across different systems and networks, the immutability of this data is of great importance when used in a hybrid cloud.



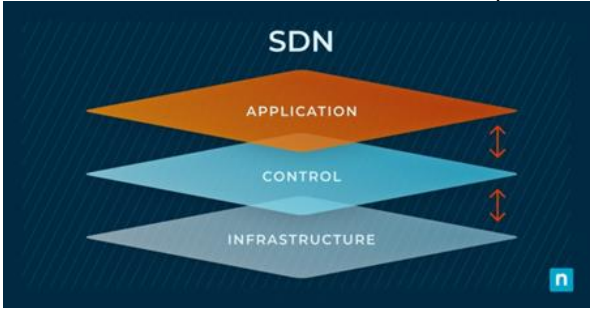
C. Edge Computing for Reduced Latency

In contrast to other computing models, edge computing involves processing that is done at the edge of networks, which reduces latency. Additionally, edge computing is more secure than other models of computing since the majority of the data does not have to traverse several networks that are not essential [2]. The risk of information being leaked during the transfer process is mitigated by processing information in this manner, and the information is maintained within clearly delineated and protected zones.



D. SDN for Dynamic Network Management

A software-defined network (SDN) can have and restore flows to control traffic and analyze real-time security issues. Since the control plane is logically isolated from the forwarding plane, SDN enables coordination of the network's control and data plane at a single point [10]. It also means it becomes easier to put and apply security measures and proactively deal with emerging threats once they are identified [1]. This means dynamic management is highly desirable in hybrid cloud environments because the network traffic pattern can be diverse



E. Role-Based Access Control (RBAC)

In the contemporary environment, RBAC is a part of even more developed IAM models and systems. It is easier to obtain resources because it depends on the particular person's authority in an organization. In addition, it strengthens protection on the employee's side and weakens the bureaucratic aspect on the employer's side.

1) RBAC for Access Management

RBAC guarantees that users are only authorized to access resources relevant to their roles in the system. Users can only request the resources required. Somasundaram et al., say that strategy helps express great control and the ability of businesses to set strict access rules and grant different permission levels to the roles without burdening the user with a minimum to no load [11].

2) Challenges and Solutions

Nonetheless, there are some issues that organizations experiencing a vast number of users have regarding RBAC implementation. Such challenges can be the use of automated role management tools and the application of complex RBAC versions, which can help eliminate the problems of large organizations during implementation [12]. It is possible to apply various automated tools to manage roles, assignments, and maintenance to minimize the role emergence issue and guarantee that the mentioned access control policies are timely and effective.

USES

Implementing edge computing, software-defined networking, and RBAC, assists in forging a solid defense for the hybrid cloud [13]. These technologies have several uses in the industry, including:

A. Financial Services

This is particularly so because, due to the nature of the business, the staff deals with cash and information about the customers, which must be preserved and kept clean. Moreover, the security of the client data is also a significant concern when offering various financial services. The findings of Taherkordi, et al. reveal that blockchain technology can produce a secure transaction record [13]. The supply of data in the Blockchain is not likely to be changed. Using edge computing reduces the time involved in the transaction [14]. On the other hand, software-defined networking (SDN) assists in regulating the traffic movement in the network in case of security threats.

B. Healthcare

First, it needs to be understood that preserving the confidentiality of the patient's information belongs to essential elements in the sphere of health care besides legal compliance. Accordingly, through the application of the Blockchain option record data can be made tamper-proof while being kept safely [15]. Also, edge computing can process such data on the device, minimizing or removing their handling entirely [15]. By adopting RBAC, it became easy for hospitals to implement extensive control measures regarding physical access to the system [16]. Such policies limit the availability of patients' data to a limited number of people in the healthcare facility.

C. Manufacturing

Protecting data traffic is essential for continuing business, security from competitors' activity, and security of data traffic generated by intelligent production networks composed of the Internet of Things devices. IoT data can also be written into a secure and well-dispersed blockchain to provide industrial data storage. While edge computing can perform data processing closer to the source, this would also mean that it takes less time to process data in the Internet of Things network [14]. SDN can control traffic distribution to prevent such organizations from infiltrating networks. RBAC can prevent personnel within a specific organization from accessing data systems that may be linked to such networks.

D. Government

Considering the requirements of national security concerns and the decisions of the population, it is necessary to apply higher levels of protection to the government's classified data and enhance the methods of access to these data. Edge computing can reduce data exposure by handling the data locally. At the same time, Blockchain can assist in preserving the safety of the data-containing appendices since they are decentralized and their transaction is unalterable [3]. Blockchain ensures the secure storage of the appendices that contain the data. It also can be used for dynamic path selection if the traffic destined to be sent can pose a security threat. Furthermore, RBAC can be beneficial in creating stricter access control policies and allowing only certain people access to a vast quantity of data.

IMPACT

The fact is that further development has intensified several-fold and drastically changed the situation, particularly in the sphere of cloud computing and the hybrid forms of cloud use. The subsequent hybrid clouds that combine private and public cloud services must advance security measures to protect the data and run efficiently. New-generation technologies like Blockchain, edge computing, Software-Defined Networking, and Role-Based Access Control play a vital role in the security of hybrid cloud networks. Such technologies present several advantages, such as more security, efficiency, and scalability.

A. Enhanced Security

Recent technologies in security systems are central to the protection of hybrid cloud solutions. Blockchain, for example, has decentralized ledgers immune to tampering that help improve privacy and data integrity. This helps eradicate the vice of data manipulation and unauthorized access since records cannot be changed once they have been made on the Blockchain [7]. It becomes beneficial in a hybrid cloud environment, especially when handling data, and the last thing one may want is a compromise.

Another advantage is Edge computing, which allows intended analysis closer to the source rather than a centralized cloud server, increasing security. Due to the reduced distance that data is transmitted, edge computing significantly decreases the probability of data interception by unauthorized subjects in transit [7]. Furthermore, with the help of software-defined networking (SDN) aspects, the network topologies can be made dynamic and programmable, thereby encouraging the usage of well-defined security policies as a solution against the latest threats. RBAC, conversely, ensures that only certain users have privileges to specific resources, minimizing insider threats and unauthorized access [7].

B. Improved Efficiency

Since hybrid cloud environments are complex, efficiency is critical when organizing cloud solutions. Edge computing and SDN offer significant improvements in managing networks and dealing with data. In effect, edge computing minimizes the latency, the time between an instruction to send data and the start of transferring the data, considering that data is processed closer to the source. This reduction in latency increases the overall efficiency of many applications and services hosted in the hybrid cloud. In addition, working data closer to the origin reduces the amount of data shuttling across networks, optimizes resource usage, and avoids overloading potential congestion areas.

SDN adds another layer to efficient operations through its feature of resource control about the dynamically changing demands. Such flexibility also helps to use different network resources effectively with little to no wastage and aids in better network performance. Meanwhile, since SDN is a software-defined network, one can program the network to provide an application or operating environment-specific security feature to complement the protection against cyber threats [7].

C. Scalability

Regarding the concept of scalability, it has emerged as one of the critical requirements for contemporary organizations that integrate hybrid cloud infrastructures. Organizations must be able to scale up these environments for the next-generation security strategies to effectively achieve their goals through conforming to the organization's IT architecture. This makes security features of blockchain systems inherently elastic to growing demand levels at a business organization while maintaining security simultaneously [7].

They also help scalability as SDN and edge computing comprise open solutions for overseeing data processing and network resources. Therefore, due to the software-defined nature of the network, incorporating the new components and tuning the existing ones to accommodate the required loads is relatively straightforward. In edge computing, data do not have to be transferred back to a central processing center at any time, making it efficient when an organization experiences growth in data traffic. These technologies offer the much-needed fluidity and extensibility for efficient and optimal control of today's advanced hybrid cloud systems [7].

SCOPE

The subject of this study comprises the theoretical foundations and the most effective practices of the next-generation security solutions implemented within the framework of hybrid cloud models. In the future, the study might investigate the following kinds of topics:

A. Advanced Blockchain Applications

Regarding the routes that subsequent research should take, examining the use of Blockchain technology to safeguard Internet of Things devices and other cutting-edge technologies is essential. Because of the characteristics of blockchain technology, it can store all of the records and verify all of the transactions on the Internet of Things networks securely and without being tampered with [17]. The merging of blockchain technology with other promising and trending technologies, such as artificial intelligence and machine learning, to improve the performance of hybrid cloud systems and provide protection for those systems is a viable topic for future research.

B. Edge Computing Innovations

The development of new edge computing compatible with the system's protection and performance. Although local processing with edge computing can significantly reduce latency and boost security, this field is still in its early stages of development [18]. The scope of this article could be expanded by adding additional resources to investigate various architectures and technologies for edge computing [19]. These include micro-edge data centers and fog computing, which can improve the prospects of a hybrid cloud.

C. Enhanced RBAC Models

To address the problems associated with large companies, steps are being taken toward the relevant next-stage RBAC [20]. Although the role-based system is challenging to organize, RBAC is suitable for large organizations since it restricts access and grants privileges [21]. Future research may study new approaches and methodologies for RBAC, such as ABAC and PBAC, to provide more sophisticated and efficient access control in the hybrid cloud.

CONCLUSION

It is recommended that hybrid cloud systems be protected based on a comprehensive methodology incorporating future-generation technology. The problems of data confidentiality, data integrity, and access rights can be reliably addressed by blockchain technology, edge computing, software-defined networking, and role-based access control [22]. The convergence of these technologies is advantageous to a company since it enhances its security, productivity, and expansiveness inside a hybrid cloud configuration. As a result, the focus of future research ought to be on the creation of additional security solutions that are capable of responding to new threats in cloud computing infrastructure.

REFERENCES

[1]. R. Montasari, R. Hill, A. H. Far, and F. Montaseri, "Countermeasures for timing-based side-channel attacks against shared, modern computing hardware," International Journal of Electronic Security and Digital Forensics, vol. 11, no. 3, pp. 294-320, 2019, doi: https://doi.org/10.1504/ijesdf.2019.100480.

[2]. W. Yu et al., "A Survey on the Edge Computing for the Internet of Things," IEEE Access, vol. 6, pp. 6900–6919, 2017, doi: https://doi.org/10.1109/access.2017.2778504.

[3]. F. Allon, "Money after Blockchain: Gold, Decentralised Politics and the New Libertarianism," Australian Feminist Studies, vol. 33, no. 96, pp. 223–243, Apr. 2018, doi: https://doi.org/10.1080/08164649.2018.1517245

[4]. S. Rathore, P. K. Sharma, V. Loia, Y.-S. Jeong, and J. H. Park, "Social network security: Issues, challenges, threats, and solutions," Information Sciences, vol. 421, pp. 43–69, Dec. 2017, doi: https://doi.org/10.1016/j.ins.2017.08.063.

[5]. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, Jan. 2011, doi: https://doi.org/10.1016/j.jnca.2010.07.006.

[6]. R. Alkadi, G. Jiang, and S. Aldamer, "A Regression Analysis of Motivations for Saudi University Male Student Volunteers," Journal of Social Service Research, vol. 45, no. 5, pp. 701–714, 2019.

[7]. V. Chaurasia, S. Pal, and B. Tiwari, "Prediction of benign and malignant breast cancer using data mining techniques," Journal of Algorithms & Computational Technology, vol. 12, no. 2, pp. 119–126, Feb. 2018, doi: https://doi.org/10.1177/1748301818756225.

[8]. Y. Wang and A. Kogan, "Designing confidentiality-preserving Blockchain-based transaction processing systems," International Journal of Accounting Information Systems, vol. 30, pp. 1–18, Sep. 2018, doi: https://doi.org/10.1016/j.accinf.2018.06.001.

[9]. B. Friedman, P. H. Kahn, A. Borning, and A. Huldtgren, "Value Sensitive Design and Information Systems," Early engagement and new technologies: Opening up the laboratory, vol. 16, pp. 55–95, 2013, doi: https://doi.org/10.1007/978-94-007-7844-3_4.

[10]. A. Abdou, P. C. van Oorschot, and T. Wan, "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 3542–3559, 2018, https://ieeexplore.ieee.org/abstract/document/8362609
[11]. S. Somasundaram, R. G. Pratt, B. Akyol, N. Fernandez, N. Foster, S. Katipamula, ... and Z. Taylor, "Reference guide for a transaction-based building controls framework." Pacific Northwest National Laboratory, 2014.
[12]. K. Abouelmehdi, A. B. Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," Journal of Big Data, vol. 5, no. 1, 2018.
[13]. A. Taherkordi, F. Zahid, Y. Verginadis and G. Horn, "Future Cloud Systems Design: Challenges and Research Directions," in IEEE Access, vol. 6, pp. 74120-74150, 2018, doi: 10.1109/ACCESS.2018.2883149.
[14]. S. Jangirala, A. K. Das and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," in IEEE Transactions on Industrial Informatics, vol. 16, no. 11, pp. 7081-7093, 2019.
[15]. T. Zhang, "Influences on healthcare providers' and parents' behaviors with respect to the use of antibiotics for children: An exploratory study in urban China," etheses.whiterose.ac.uk, Sep. 06, 2018.
[16]. S. J. Dancer, "Controlling Hospital-Acquired Infection: Focus on the Role of the Environment and New Technologies for Decontamination," Clinical Microbiology Reviews, vol. 27, no. 4, pp. 665–690, Oct. 2014, doi: https://doi.org/10.1128/cmr.00020-14.
[17]. G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A Blockchain Framework for Securing Connected and Autonomous Vehicles," Sensors, vol. 19, no. 14, p. 3165, Jul. 2019, doi: https://doi.org/10.3390/s19143165.
[18]. C. A. Gilligan, "Sustainable agriculture and plant diseases: an epidemiological perspective," Philosophical Transactions of the Royal Society B: Biological Sciences, vol. 363, no. 1492, pp. 741–759, Sep. 2008, doi: https://doi.org/10.1098/rstb.2007.2181.
[19]. P. Mach and Z. Becvar, "Mobile Edge Computing: A Survey on Architecture and Computation Offloading," in IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1628-1656, thirdquarter 2017, doi: 10.1109/COMST.2017.2682318.
[20]. F. Nazerian, H. Motameni, and H. Nematzadeh, "Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy," Journal of Information Security and Applications, vol. 45, pp. 131–142, Apr. 2019, doi: https://doi.org/10.1016/j.jisa.2019.01.008.
[21]. T. Rabehaja, S. Pal, and M. Hitchens, "Design and implementation of a secure and flexible access-right delegation for resource constrained environments," Future Generation Computer Systems, vol. 99, pp. 593–608, Oct. 2019, doi: https://doi.org/10.1016/j.future.2019.04.035.
[22]. P. Raj and M. Periasamy, "The Convergence of Enterprise Architecture (EA) and Cloud Computing," Computer Communications and Networks, pp. 61–87, 2011, doi: https://doi.org/10.1007/978-1-4471-2236-4_4.