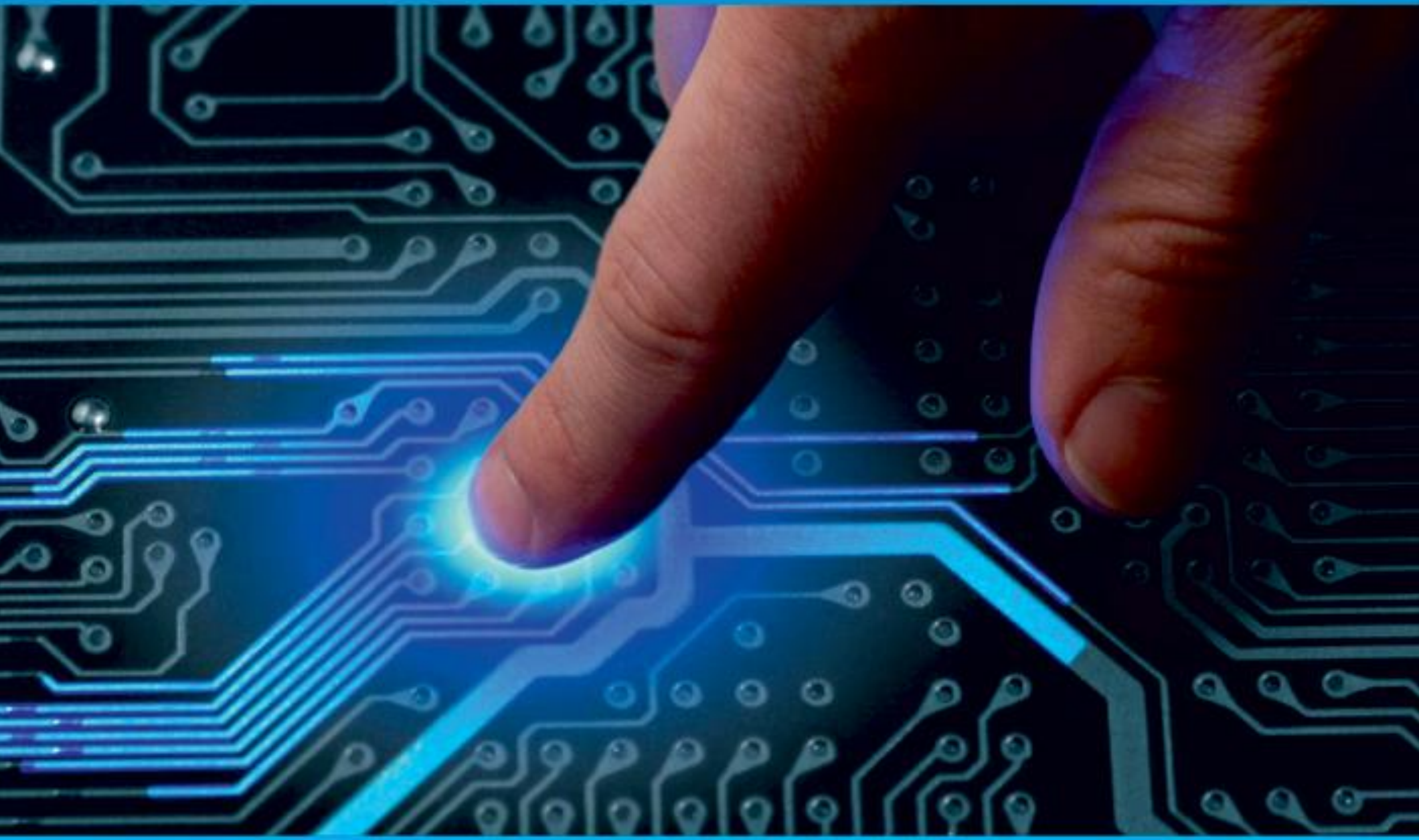
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1205185 |

A Research on Hybrid Cloud Computing

B Mahaswarup, Bhuvana J

PG Student, Department of C.S & I.T, Jain (Deemed to be University), Bangalore, India

Professor, Department of C.S & I.T, Jain (Deemed to be University), Bangalore, India

ABSTRACT: Dual distributed computing has arisen as a significant answer for present day ventures trying to use the benefits of both public and confidential cloud foundations. This theoretical digs into the pith of crossover distributed computing, inspecting its design, advantages, challenges, and arising patterns molding its reception. Cross breed cloud engineering consistently incorporates public and confidential cloud conditions, permitting associations to improve responsibility position in view of elements like security, consistence, execution, and cost-proficiency. By mixing the versatility and adaptability of public mists with the control and customization of private mists, dual models engage endeavors to draftsman modern IT environments custom-made to their extraordinary necessities. The advantages of mixed distributed computing are complex. Associations can powerfully scale assets, moving responsibilities between conditions to successfully oblige vacillations sought after. Furthermore, mixture mists work with information sway, empowering endeavors to hold delicate information on-premises while utilizing the dexterity of public mists for less basic responsibilities. This flexibility encourages development and speeds up computerized change drives, enabling organizations to remain deft and serious in a quickly developing scene. In any case, hybrid cloud reception likewise presents difficulties. Overseeing different cloud conditions presents intricacy, requiring powerful administration structures, robotization devices, and gifted faculty to guarantee consistent organization and security across the mixture framework. Interoperability issues, information coordination concerns, and potential seller secure in additional highlight the significance of fastidious preparation and vital dynamic in crossover cloud arrangements. Looking forward, a few patterns are reshaping the hybrid cloud scene. Edge registering is acquiring conspicuousness, driving the decentralization of information handling and stockpiling to the organization edge, subsequently enlarging mixed models with edge capacities. Besides, progressions in containerization advances, like Kubernetes, are working with compactness and responsibility portability across mixed conditions, upgrading spryness and asset use. All in all, dual distributed computing addresses a change in outlook in IT framework the executives, offering a strong mix of adaptability, versatility, and control. While reception involves difficulties, the essential reconciliation of public and confidential mists can open unmatched open doors for advancement and effectiveness in the computerized time. Embracing mixed cloud structures enables undertakings to explore intricacy, mitigate risk, and benefit from arising advancements to drive feasible development and upper hand.

KEYWORDS: Hybrid Cloud, Private Cloud, Public Cloud, Scalability, Edge Computing.

I. INTRODUCTION

In the present advanced scene, organizations are continually looking for ways of upgrading their IT foundation to improve dexterity, adaptability, and cost-proficiency while keeping up with severe security and consistence principles. In the midst of this pursuit, amalgamated distributed computing has arisen as a convincing arrangement, offering associations the smartest scenario imaginable via consistently incorporating public and confidential cloud conditions. Amalgamated distributed computing addresses an essential way to deal with IT design that joins the advantages of on-premises framework with those of public cloud administrations. This model permits undertakings to use the versatility, adaptability, and cost-viability of public mists while holding command over delicate information and basic responsibilities inside confidential cloud or on-premises conditions. At its center, amalgamated cloud engineering works with responsibility convenience and information versatility across various conditions, empowering associations to progressively allot assets in view of responsibility prerequisites, execution targets, and administrative contemplations. By utilizing an amalgamated approach, organizations can accomplish more prominent flexibility, versatility, and proficiency, all while limiting expenses and improving asset use. The idea of amalgamated distributed computing has built up some momentum across enterprises because of its capacity to address a heap of IT challenges. For example, associations with inheritance frameworks or severe consistence necessities might pick to keep up with basic jobs on-premises while utilizing public mists for non-delicate undertakings or bursty responsibilities during top interest periods. Likewise, organizations working in profoundly controlled areas, like money or medical services, can profit from the adaptability to store delicate information on confidential mists while using the versatility of public mists for less touchy tasks. Besides, amalgamated cloud structures empower endeavors to embrace arising advancements, for example, edge processing and containerization, subsequently broadening the span of their framework and opening new open doors for development and development. By decisively incorporating public and confidential cloud assets, associations can construct versatile, dexterous, and future-evidence IT biological systems fit for adjusting to developing business needs and innovative headways. Be that as it may, while amalgamated distributed computing offers various advantages, its reception likewise presents difficulties. Overseeing dissimilar cloud conditions, guaranteeing consistent coordination and interoperability, and keeping up with reliable security and consistence norms across amalgamated foundations require cautious preparation, hearty administration systems, and gifted staff. In rundown, amalgamated distributed computing addresses an extraordinary way to deal with IT foundation the executives, offering associations the adaptability, versatility, and control expected to flourish in the present unique business climate. By saddling the force of amalgamated structures, undertakings can speed up advancement, drive effectiveness, and open new open doors for development while relieving risk and expanding the worth of their IT ventures.

II. METHODOLOGIES AND RESEARCH TECHNIQUES

Implementing hybrid cloud computing involves integrating and managing resources across multiple cloud environments, including public clouds, private clouds, and on-premises infrastructure. Several methodologies and strategies are commonly used to implement hybrid cloud computing effectively

Cloud Bursting: This methodology involves dynamically allocating workloads between a private cloud and a public cloud during peak demand periods. Applications run in the private cloud under normal circumstances, but when additional resources are required, they "burst" into the public cloud to handle the increased load.

API Integration: APIs (Application Programming Interfaces) are essential for connecting and integrating different cloud environments. By utilizing APIs provided by cloud service providers, organizations can create a unified management interface for hybrid cloud resources, enabling seamless interaction and data transfer between environments.

Orchestration and Automation: Orchestration tools automate the provisioning, configuration, and management of hybrid cloud resources. By defining workflows and policies, organizations can streamline deployment processes, optimize resource utilization, and ensure consistency across hybrid environments. Tools like Kubernetes, Terraform, and Ansible are commonly used for orchestration and automation.

Software-Defined Networking (SDN): SDN technologies abstract network infrastructure, allowing organizations to create virtualized, programmable networks that span multiple cloud environments. SDN enables centralized management, dynamic resource allocation, and secure connectivity between on-premises data centers and public clouds, facilitating hybrid cloud deployments.

Data Management and Governance: Effective data management is crucial for hybrid cloud environments, ensuring data consistency, security, and compliance across diverse platforms. Data governance policies define rules and procedures for data access, storage, and usage, while data integration tools facilitate seamless data movement between on-premises and cloud environments.

Identity and Access Management (IAM): IAM solutions manage user identities and access permissions across hybrid cloud environments, ensuring secure authentication and authorization mechanisms. Centralized IAM platforms provide unified identity management, enforcing consistent security policies and access controls regardless of the cloud environment.

Hybrid Cloud Management Platforms (CMPs): CMPs offer comprehensive management capabilities for hybrid cloud environments, including resource provisioning, monitoring, cost optimization, and workload migration. These platforms provide a single pane of glass for managing hybrid infrastructure, simplifying operations and improving overall efficiency.

Security and Compliance: Hybrid cloud security encompasses various measures, including encryption, firewalls, intrusion detection/prevention systems, and security information and event management (SIEM) solutions. Additionally, compliance frameworks such as GDPR, HIPAA, and PCI DSS must be adhered to across all cloud environments to ensure regulatory compliance and data protection.

III. HYBRID CLOUD ARCHITECTURE

Public clouds are traditionally hardware, network, storage, and computing resources owned and maintained by third-party vendors. Though using a public cloud does offset the cost of setting up on-premise infrastructure from scratch, it comes with its own pitfalls. Organizations often face a lack of data visibility when it comes to public clouds. Public cloud vendors and their users work on a 'shared responsibility' model, which means that organizations are responsible for most of the security aspects. Add in compliance regulations, and it becomes crucial that organizations have a strong hold on how and where their systems are running.

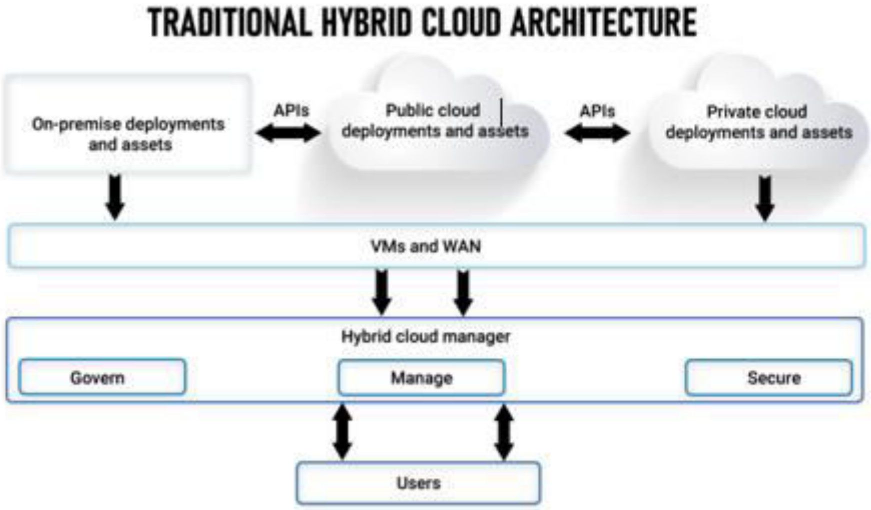

TRADITIONAL HYBRID CLOUD ARCHITECTURE
On-premise deployments and assets
APIs
Public cloud deployments and assets
APIs
Private cloud deployments and assets
VMs and WAN
Hybrid cloud manager
Govern
Manage
Secure
Users

Fig 1: Traditional Hybrid Cloud Architecture

This is why more and more organizations are opting for private cloud models. Private cloud may be an entire data center that is deployed, operated, and maintained on-premise. This requires a lot of capital. Another option is using rented, vendor-owned data centers that are off-premise. AWS, Google Cloud, and Azure each provide their own private cloud solutions. Vendor-driven public clouds are shared with other users (though one customer's data is hidden from another), while a vendor-owned private cloud is specific to an organization and involves no sharing. Though they do provide more control, private clouds are more expensive than public clouds.

All applications and data owned by an organization do not have the same requirements in terms of space, computation, security, and compliance. While some operations such as email and file sharing can be hosted on a public cloud, proprietary operations and sensitive customer data would be more secure in an on-premise or private cloud setup. This is where the hybrid cloud comes in.

A hybrid cloud aims to make a single, flexible infrastructure that connects various workloads running in different computational environments. If done right, IT admins and DevOps teams will be able to access and maintain their systems and data through one hybrid cloud management console. In other words, separate clouds become hybrid when there's a level of orchestration between them.

IV. DISCUSSIONS

A. Experimental Setup

For training and validating the detection accuracy of a threat classification and anomaly detection model, a substantial amount of data is required. Unfortunately, publicly available network traffic datasets have numerous flaws. They are frequently erroneous, out of date, or lack the proper labels. Common network protocol issues include hiding or not addressing features, insufficient variety and volume of traffic, and inadequate coverage of known threats. In order to address these concerns, the Canadian Institute of Cyber-security created the CICIDS 2017 dataset in 2017 . This dataset is noteworthy because it meets all eleven standards for an IDS dataset. This dataset is intended to be as near to real - world data as feasible by including both benign traffic and the most current prevalent attacks. The CICIDS 2017 benchmark dataset tracks the attack behaviors of 25 users across multiple protocols, including email, SSH, FTP, HTTP, and HTTPS. Preprocessing methods such as data balancing, normalizat ion, and categorical encoding were performed to make the dataset more acceptable for attack classification and detection models. The balanced dataset, shown in Table 1, shows the distribution of "Attack" and "Normal" samples across the testing and training sets.

Table 1. Balanced CICIDS 2017 dataset

DATASET	TRAIN	SET
ATTACK	1500	500
NORMAL	1500	500
TOTAL	3000	1000

B. DL Model Outcome

Using the CICIDS 2017 dataset, we assessed the significance of the proposed hybrid framework in increasing cloud data security. For comparison, two more DL models, LSTM and CNN, were used. Tables 1, 2, and 3 show the classification results for each model as represented by the confusion matrices. Looking at the CNN confusion matrix, we can observe that the model correctly identified 479 attacks (True Positives-TP) while incorrect ly identifying 482 normal behaviors (True Negatives -TN). However, there were 22 False Positives (FP), which occurred when harmless behavior was misinterpreted for an attack, and 17 False Negatives (FN), which occurred when attacks were actually missed.

Table 2. Confusion matrix of CNN

ACTUAL CLASS	PREDECTION CLASS	
	ATTACK	NORMAL
ATTACK	479	22
NORMAL	17	482

According to the confusion matrix, LSTM had 492 TN and 486 TP. Furthermore, 9 legit imate attacks were unnoticed, and 13 incidents of benign activity were mislabeled as attacks.

Table 3. Confusion matrix of LSTM

ACTUAL CLASS	PREDECTION CLASS	
	ATTACK	NORMAL
ATTACK	486	13
NORMAL	9	492

The confusion matrix of the Hybrid Model performs better, with 497 TP and 495 TN. Only 6 instances of normal behavior were misclassified as attacks, while two instances of malicious activity went unnoticed.

Table 4. Confusion matrix of LSTM

ACTUAL CLASS	PREDECTION CLASS

	ATTACK	NORMAL
ATTACK	497	6
NORMAL	2	495

Table 5 offers performance metrics that evaluate the usefulness of three models—CNN, LSTM, and the proposed Hybrid Model—in increasing data security in cloud environments using the CICIDS 2017 dataset. CNN achieved an accuracy of 96.1%, LSTM showed a slight improvement with an accuracy of 97.8%, and the Hybrid Model, on the other hand, obtained a stunning 99.2% accuracy, much exceeding either of the other models. The LSTM achieved a detection rate of 97.394%, whereas CNN achieved a rate of 95.608%. The Hybrid Model has the highest capability to correctly identify attacks, with a detection rate of 98.807%.CNN had a false alarm rate of 3.406%, the LSTM output was 1.796%, and the Hybrid Model was only 0.402%. The LSTM achieved 98.181% precision, whereas CNN achieved 96.572% and the Hybrid Model stood out with a 99.599% precision score.

Table 5. Performance evaluation of model on Attack Detection

MODEL	CNN	LSTM	HYBRID
Accuracy	96.1	97.8	99.2
Detection Rate	95.608	97.394	98.807
False Alarm Rate	3.406	1.796	0.402
Precision	96.572	98.181	99.599

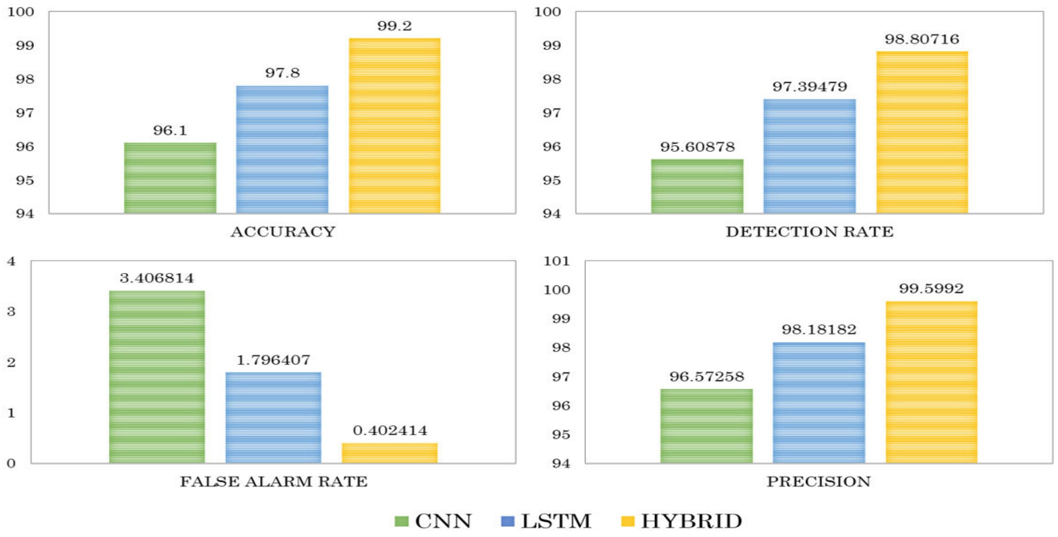


Chart 1: Discussions About Setup

V. CONCLUSION

In conclusion, hybrid cloud computing represents a transformative paradigm in IT infrastructure management, offering organizations unparalleled flexibility, scalability, and control to meet the dynamic demands of the digital age. Through the strategic integration of public and private cloud environments, hybrid cloud architectures empower businesses to optimize resource utilization, enhance agility, and drive innovation while addressing key challenges such as security, compliance, and cost management.

Hybrid cloud computing enables organizations to leverage the scalability and cost-effectiveness of public clouds for non-sensitive workloads while retaining control over critical data and applications within private or on-premises environments. This flexibility allows businesses to adapt quickly to changing workload requirements, scale resources dynamically, and capitalize on emerging technologies such as edge computing and containerization.

Moreover, hybrid cloud architectures facilitate seamless workload portability, data mobility, and interoperability across heterogeneous environments, enabling organizations to maximize efficiency and productivity. By harnessing advanced orchestration, automation, and analytics capabilities, businesses can optimize performance, mitigate risks, and drive continuous improvement in their hybrid cloud deployments.

However, the adoption of hybrid cloud computing also presents challenges, including managing complexity, ensuring security and compliance, and navigating vendor lock-in. Addressing these challenges requires robust governance frameworks, advanced security controls, and strategic planning to align hybrid cloud initiatives with business objectives and regulatory requirements.

Looking ahead, the future of hybrid cloud computing promises further enhancements in orchestration, automation, security, and interoperability, driven by advancements in AI, edge computing, containerization, and multi-cloud integration. By embracing these trends and leveraging collaborative research efforts, organizations can unlock new opportunities for innovation, efficiency, and growth in the evolving digital landscape.

REFERENCES

[1] S. Rekha, Manish Sharma, Sathish Kannan, Vijay Jagdish Upadhye, Harshal Patil, & S. Rajkumar. (2024). Hybrid Deep Learning Approaches for Data Security in Cloud Environments. *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT).* https://doi.org/10.1109/idciot59759.2024.10467848

[2] Ming-Yen Wu, Chung-Jhih Tsai, Wan-Ting Su, Sian Ciou, Yu-Shuo Lee, & Chien-Hua Lee. (2023). Hybrid Cloud Energy Management for Edge Computing. *2023 International Conference on Consumer Electronics - Taiwan (ICCE-Taiwan).* https://doi.org/10.1109/icce-taiwan58799.2023.10226741

[3] Jayaudhaya J, Jayaraj R, & Ramash Kumar K. (2024). A New Integrated Approach for Cloud Service Composition and Sharing Using a Hybrid Algorithm. *Mathematical Problems in Engineering*, *2024*, 1–11. https://doi.org/10.1155/2024/3136546

[4] V Ananthakrishna, Shekhar Chandra, & Yadav. (2023). *Migration Letters Advancements in Cloud Security: An Enhanced Auth Privacy Chain-Based*
Hybrid Encryption Technique for Scalability 486 Advancements in Cloud Security: An Enhanced Auth Privacy Chain-Based Hybrid Encryption Technique for Scalability. *S13*, 1741–8992.

[5] Rima Akter, Md. Ashikur Rahman Khan, Fardowsi Rahman, Sultana Jahan Soheli, & Nusrat Jahan Suha. (2023). RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing. *International Journal of Computational and Applied Mathematics & Computer Science*, *3*, 60–71. https://doi.org/10.37394/232028.2023.3.8

[6] HuitingWei. (2022). Optical Hybrid Network Structure Based on Cloud Computing and Big Data Technology. *Journal of Sensors*, *2022*, 1–6. https://doi.org/10.1155/2022/3936876

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details