IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Robust Database Protection: Combining Quantum Key Distribution, Blockchain, Honeypots, TDE and AES Encryption

Akshatha Kamath[1], Priya K[1], Risshab Srinivas Ramesh[2]

Assistant Professor, Department of Computer Science & Engineering, Ramaiah Institute of Technology, Bengaluru, Karnataka, India[1]

B. E Student, Department of Computer Science & Engineering, Ramaiah Institute of Technology, Bengaluru, Karnataka, India[2]

ABSTRACT: A lot of threats are faced by modern database security which depends on encryption and control. In this regard, the Quantum Key Distribution (QKD) is recommended as an effective remedy which relies upon quantum mechanics' basic principles to ensure absolute security. Furthermore, it investigates integrating Field-Programmable Gate Arrays (FPGAs) to expedite cryptographic operations, enhancing the overall security framework. By combining the resilience of QKD and the computational efficiency of FPGAs, this research offers a comprehensive strategy to secure databases against threats and evolving cyber risks. Additionally, the integration of blockchain technology can provide an immutable and decentralized record of transactions, enhancing the transparency and auditability of database operations. This proactive and adaptable defence in the rapidly evolving technological landscape ensures robust security against emerging threats and cyber risks.

KEYWORDS: QKD, FPGA, Blockchain Technology, Honeypot, AES, Transparent Data Encryption, DLT

I. INTRODUCTION

In the contemporary data-driven landscape, ensuring the protection of sensitive information stored within databases is paramount. A single breach has the potential to expose financial records, customer data, intellectual property, and other critical assets, leading to severe consequences. This research delves into the crucial realm of database security, examining essential measures employed to safeguard valuable data effectively. This paper elucidates on five overarching measures aimed at enhancing the security posture of databases.

1. Transparent Data Encryption (TDE): Encodes information base records very still, safeguarding information regardless of whether actual media is taken.
2. Blockchain Technology: To maintain the information unchangeable and prevent illegal alterations, a distributed ledger records all database transactions which are made in an immutable manner.
3. Honeypots: Deploy decoy systems that mimic real databases to attract and trap attackers, revealing their tactics and techniques.
4. Advanced Encryption Standard (AES): Employs a symmetric encryption algorithm to secure data both at rest and in transit.
5. Quantum Key Distribution (QKD): Quantum Key Distribution (QKD) is a cryptographic protocol that leverages the principles of quantum mechanics to securely exchange encryption keys between two parties.

Transparent Data Encryption (TDE) provides strong data protection at rest but can impact performance. Blockchain Technology ensures data integrity and immutability but can be complex to implement. Honeypots offer insights into attacker behaviour but may not be effective against sophisticated threats. AES provides robust encryption for both data at rest and in transit but requires secure key management. Quantum Key Distribution offers theoretically unbreakable

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

encryption but requires specialized hardware and infrastructure. The best choice of technique depends on factors like data sensitivity, risk assessment, and available resources.

II. METHODOLOGY

A. Blockchain for Database Security

Blockchain can be defined as a decentralized, immutable, and transparent digital ledger that records transactions across multiple computers or nodes. Unlike traditional centralized systems, Blockchain operates on a peer-to-peer network, where every participant has access to a copy of the entire ledger. This distributed nature ensures that no single entity has control over the network, making it highly secure and resistant to tampering.

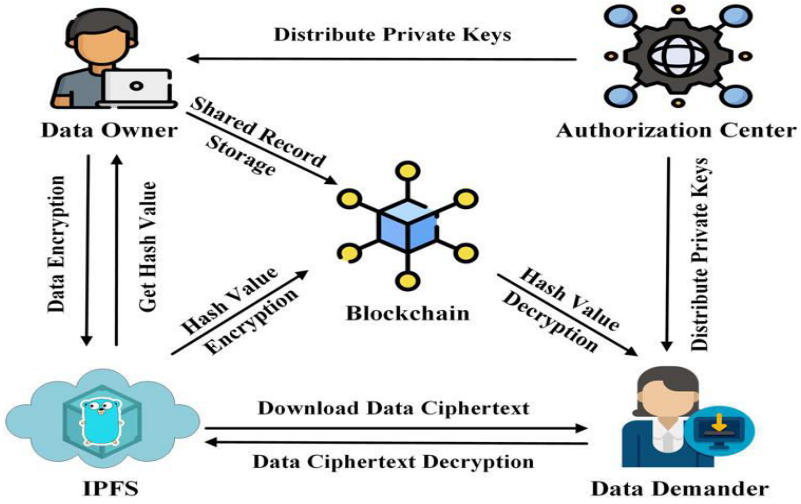

FIG 1: A blockchain-based traceable and secure data-sharing scheme (Copyright: PeerJ computer science Journal)

Databases store critical information across various sectors. Wireless backup is crucial in our increasingly connected world, where data loss can lead to significant financial losses and security breaches. Traditional wireless backup solutions rely on centralized servers or data centres, which come with inherent vulnerabilities. These centralized systems are susceptible to cyberattacks, hardware failures, and natural disasters. Blockchain technology, with its distributed and tamper-proof ledger system, presents a paradigm shift in data security.

Current research challenges include:

1. Scalability: Blockchain networks can be slow and inefficient due to the high computational requirements for validating transactions, which strain the system as the number of users, transactions, and applications increases. This makes it challenging to process and validate transactions promptly, particularly in situations demanding fast transaction speeds. The significant computational burden during validation leads to substantial latency issues, further exacerbated by the growing number of users on platforms like social media and voice assistants. Consequently, the increasing demands overwhelm blockchain systems, hindering real-time applications like instant payment processing in games.
2. Privacy: Balancing transparency with data privacy remains a challenge, requiring innovative solutions like zero-knowledge proofs.
3. Interoperability: Interoperability, or the ability of different blockchain networks to communicate and interact with each other, is another crucial challenge facing the industry. This makes it less interoperable, and it can create inconvenience as users may be obliged to work in various platforms and may need to use different tokens or cryptocurrencies to interact with several other networks. It can also lead to disconnection between the ecosystem networks and individuals and organizations that utilize blockchains, impede communication among them, and reduce the ability to share information and value flows seamlessly.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Complexity: The technology of the establishment of blockchain is deep and requires the input of highly skilled professionals to blend it into the right mainstream system. Some technology issues that are associated with the use of blockchain may slow down the extent of its usage and discourage persons from going for the chain.

While still in its nascent stages, blockchain offers a revolutionary approach to database security. Its distributed, tamper-proof, and auditable nature presents a compelling alternative to traditional centralized systems. Research is actively addressing scalability, privacy, and regulatory concerns, paving the way for wider adoption and integration with existing database technologies. Blockchain's potential to enhance data security holds immense promise for various sectors, from finance and healthcare to supply chain management and government services.

Distributed Ledger Technologies:
Blockchain was first used in financial transactions, but as it developed, sectors and researchers investigated its many uses. New distributed technology variations have arisen because of the benefits and limitations of Blockchain, giving rise to the idea of Distributed Ledger Technology (DLT).

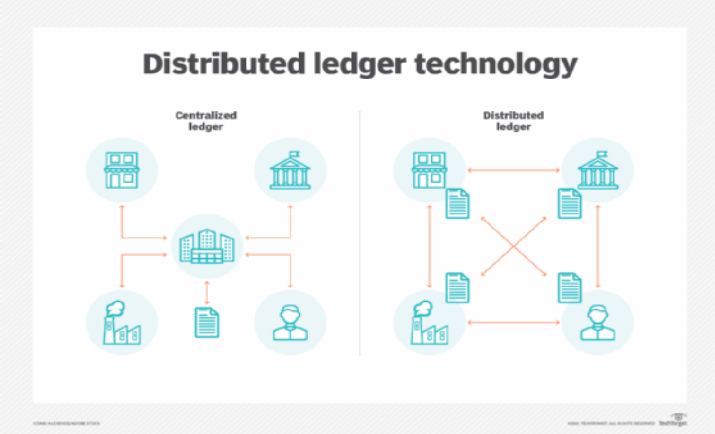

Fig 2: Distributed Ledger Technology (Copyright: TechTarget)

DLT applications can enhance dispersed environments' immutability, transparency, and traceability.

Ways to improve data security using DLT:
1. Immutability: Data is essentially unchangeable once it is stored on the DLT. Since cryptographic hashing and consensus procedures are used, it is very impossible to change or tamper with previous data.
2. Mechanisms of Consensus: To validate transactions, DLT uses consensus techniques like Proof of Work (PoW), Proof of Stake (PoS), or other algorithms. By guaranteeing that every node in the network agrees with the ledger's status, this consensus improves the data's overall security.
3.Encryption: To secure data, DLT frequently uses cryptographic methods. Sensitive data is encrypted both during transmission and at rest to make it more difficult for unauthorized parties to access or intercept.

B. Honeypots
In cybersecurity honeypots are fake or simulated targets are placed near the real targets an organization uses for actual work. Honeypots appear as attractive targets, and they can actually be deployed in a way that makes the IT in charge of the system follow the security responses of the system and in the process, guide the attacker away from target.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

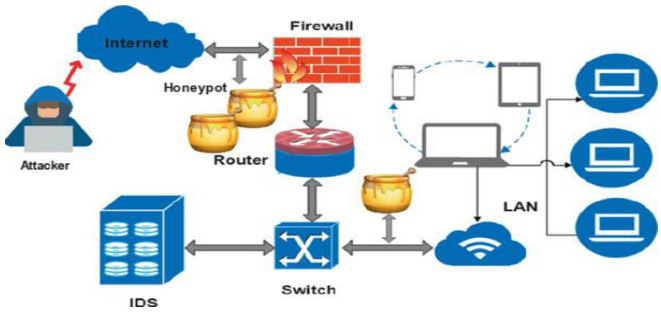

Fig 3: Multi-platform Honeypot for Capturing Real-time Cyber Attacks (Copyright: Springerlink)

Honeypots are rapidly transforming into sophisticated traps for database attackers. Some of the key areas that are boosting their effectiveness is mentioned below:

1. Hyper-Realistic Deception: Today's honeypots aren't mere static replicas. They pulsate with dynamic data, mimic real-world applications with AI-driven behaviour, and even sport carefully seeded vulnerabilities, all to convincingly lure and expose even the most cunning adversaries.
2. Proactive Defence Beyond Detection: Beyond simply identifying attackers, advanced honeypots are integrated into broader honeynet setups, enabling real-time threat assessment and automated countermeasures. This dynamic feedback loop provides deeper insights into attack patterns and empowers proactive defence mechanisms.
3. Taming the Thorny Issues: Honeypots are evolving to address critical concerns like privacy. Secure data handling techniques ensure legitimate user activity isn't compromised. Additionally, legal compliance measures are carefully considered to avoid unintended consequences. Furthermore, continuous updates keep honeypots abreast of the ever-shifting threat landscape.

C. Quantum Cryptography

Quantum cryptography can therefore be described as a sub-discipline of practical cryptography that uses theory of quantum mechanics in order to augment security of the transmitted data. The final distinct between this form of cryptography and the other is that while classical cryptography works on the basis of how hard it is to solve mathematical problems, quantum cryptography works with Quantum Mechanics to assure security of communication channels. What has happened is that quantum cryptography can also be described in terms of two basic stages, namely, to generate cryptographic keys using quantum states and to distribute these keys.

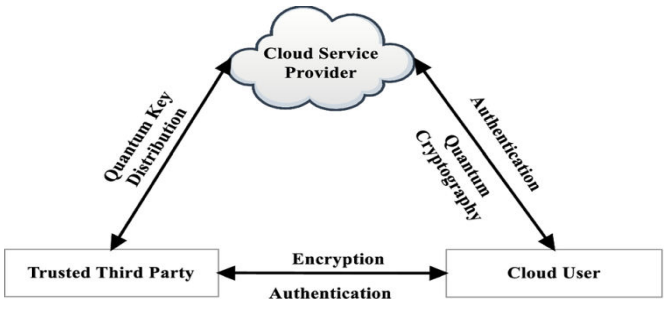

Fig 4: Quantum cryptography in cloud data computing (Copyright: Researchgate.net)

Quantum Cryptography typically involves the following elements:
1. Quantum Superposition: Quantum particles, such as photons, can exist in multiple states simultaneously, known as superposition. This property allows the encoding of multiple bits of information in a single quantum state.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

2. Quantum Entanglement: Entanglement is a phenomenon where two or more particles become correlated in such a way that the state of one particle is directly related to the state of the other(s). Changes to the state of one entangled particle instantaneously affect the state of the others, regardless of the distance between them.
3. Quantum Key Distribution (QKD): QKD is a key component of quantum cryptography. It enables two parties, traditionally referred to as Alice and Bob, to create a shared secret key over a quantum communication channel. The process involves sending quantum states (usually photons) and using the principles of quantum mechanics to detect any eavesdropping attempts.
4.BBM92 (BB84) Protocol: The BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984, is one of the earliest and most well-known quantum key distribution protocols. It uses the principles of quantum superposition and uncertainty to create a secure key.

D. Transparent Data Encryption
Transparent Data Encryption (TDE) has become a cornerstone of database security in recent years. It encrypts data at rest, rendering it unreadable to unauthorized actors even if they gain physical access to the storage media. This survey delves into the existing research on TDE, exploring its benefits, limitations, and various implementation perspectives.

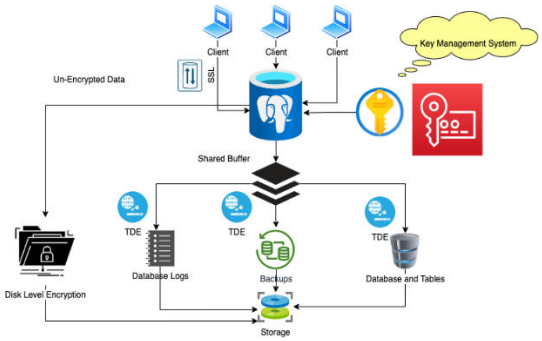

Fig 5: Transparent Data Encryption (Copyright: Percona)

Benefits of TDE:
1. Enhanced Data Security: The primary benefit of TDE is enhanced data security. By encrypting data, it renders it unreadable to anyone without the decryption key, significantly reducing the risk of data breaches and unauthorized access.
2. Compliance Adherence: TDE helps organizations comply with various data protection regulations like HIPAA, PCI DSS, and GDPR by safeguarding sensitive information.

E. AES Algorithm
AES is an example of a set of symmetric-key cryptography standards increasing confidentiality of information and data. Database security is paramount in today's digital world, where sensitive information is increasingly stored and processed. Encryption plays a vital role in safeguarding databases, particularly through algorithms like AES. This paper investigates the use of AES in database security, analysing its capabilities and limitations.

While AES stands as a robust encryption algorithm, its traditional approach involves decrypting data before performing computations, potentially exposing sensitive information. Homomorphic encryption (HE) offers a groundbreaking solution by enabling computations directly on encrypted data, keeping it protected even during processing.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. RESULT AND DISCUSSION

Table 1. Blockchain vs Existing security mechanisms

Parameter	Blockchain	Existing security mechanisms
Immutability:	Data recorded on a blockchain is tamper-proof due to its distributed ledger and cryptographic hashing.	Traditional databases can be altered, potentially leaving false audit trails and compromising data integrity.
Decentralization:	No single entity controls the data, mitigating risks of centralized attacks and data breaches.	Traditional databases have central administration points, making them vulnerable to single points of failure.
Transparency:	All transactions are publicly visible on the blockchain, promoting accountability and facilitating auditing.	Access logs and audit trails in traditional databases may be less transparent or prone to manipulation.
Fault Tolerance:	Distributed nature ensures data accessibility even if individual nodes fail, enhancing resilience against outages.	Traditional databases rely on centralized servers, making them susceptible to single points of failure.
Scalability:	Scalability remains a challenge for many blockchain implementations, potentially impacting performance with large datasets.	Traditional databases can readily scale by adding server capacity, offering better performance for high-volume transactions.
Cost and Complexity:	Implementing and maintaining blockchain infrastructures can be complex and expensive, especially for smaller organizations.	Traditional database solutions are generally more established and cost-effective, though advanced security features often come at a premium.

Table 2. Honeypot vs Existing security mechanisms

Parameter	Existing TDE	FPGA Incorporated TDE
Hardware Implementation	Implemented in software, relying on the database server's CPU for encryption/decryption operations.	Leverages Field Programmable Gate Arrays (FPGAs) for hardware-accelerated encryption/decryption.
Performance	Can introduce performance overhead due to CPU-bound encryption/decryption processes.	Offers significantly faster encryption/decryption speeds due to FPGA's parallel processing capabilities.
Flexibility	Software-based, offering flexibility in algorithm selection and configuration.	Requires hardware configuration, potentially limiting algorithm choices and customization options.
Security	Relies on software-based security measures, potentially vulnerable to software attacks.	Offers enhanced security due to hardware isolation and reduced attack surface.
Cost	Requires no additional hardware costs.	Involves the cost of FPGA hardware and integration efforts.
Complexity	Relatively easier to implement and manage within database systems.	Requires expertise in FPGA programming and integration with database infrastructure.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 3. Existing TDE vs FPGA incorporated TDE

Parameter	Honeypot	Existing security mechanisms
Proactive Defence:	Actively entice attackers, revealing their tactics and tools before they breach real systems.	Primarily react to suspicious activity, potentially allowing damage before detection.
Threat Intelligence:	Provide rich data on attacker behavior, methodologies, and tools, informing future defense strategies.	Usually generate generic alerts, requiring further analysis for actionable intelligence.
Resource Diversion:	Consume attacker time and resources, keeping them occupied away from genuine databases.	Focus on blocking or slowing down attacks, not necessarily diverting attackers entirely.
Decoy and Distraction:	Mimic real systems, misleading attackers and wasting their efforts on non-critical data.	Primarily protect actual databases, offering limited deception tactics.
Implementation Complexity:	Setting up and maintaining realistic honeypots requires specialized expertise and continuous updates.	Often come as software packages or are built-in features, simplifying deployment.
False Positives and Legal Concerns:	May attract unintended attention or trigger legal issues depending on target vulnerabilities and data types.	False positives can disrupt operations and waste resources, requiring careful configuration.

IV. CONCLUSION

In conclusion, the combination of Transparent Data Encryption (TDE), Blockchain technology, Honeypots, and Advanced Encryption Standard (AES) offers a robust and comprehensive approach to securing data. TDE ensures that data remains encrypted at rest, safeguarding against unauthorized access even if physical storage is compromised. Blockchain enhances data integrity and immutability, providing a tamper-proof ledger for transparent and auditable transactions. Honeypots serve as decoys to lure and identify potential attackers, strengthening overall security posture. AES, with its strong encryption algorithm, fortifies data transmission and storage, adding an extra layer of protection against cyber threats. Combined, these technologies make a strong frontline of defense against the threats that can compromise databases, requiring further protection of the sensitive information in today's ever growing digital environments.

REFERENCES

[1] Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. "Blockchain challenges and opportunities: A survey." International journal of web and grid services 14, no. 4 (2018): 352-375.
[2] Ali, Omar, Ashraf Jaradat, Atik Kulakli, and Ahmed Abuhalimeh. "A comparative study: Blockchain technology utilization benefits, challenges and functionalities." Ieee Access 9 (2021): 12730-12749.
[3] Wohrer, Maximilian, and Uwe Zdun. "Smart contracts: security patterns in the ethereum ecosystem and solidity." In 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE), pp. 2-8. IEEE, 2018.
[4] Jiao, Jiao, Shuanglong Kan, Shang-Wei Lin, David Sanan, Yang Liu, and Jun Sun. "Semantic understanding of smart contracts: Executable operational semantics of solidity." In 2020 IEEE Symposium on Security and Privacy (SP), pp. 1695-1712. IEEE, 2020.
[5] Steichen, Mathis, Beltran Fiz, Robert Norvill, Wazen Shbair, and Radu State. "Blockchain-based, decentralized access control for IPFS." In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1499-1506. IEEE, 2018.
[6] Truong, Nguyen, Gyu Myoung Lee, Kai Sun, Florian Guitton, and YiKe Guo. "A blockchain-based trust system for decentralized applications: When trustless needs trust." Future Generation Computer Systems 124 (2021): 68-79.
[7] Merrell, Ian. "Blockchain for decentralized rural development and governance." Blockchain: Research and Applications 3, no. 3 (2022): 100086.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[8] Basegio, Tulio L., Regio A. Michelin, Avelino F. Zorzo, and Rafael H. Bordini. "A decentralized approach to task allocation using blockchain." In Engineering Multi-Agent Systems: 5th International Workshop, EMAS 2017, São Paulo, Brazil, May 8-9, 2017, Revised Selected Papers 5, pp. 75-91. Springer International Publishing, 2018.
[9] Nizamuddin, N., & Abugabah, A. (2021). Blockchain for automotive: An insight towards the IPFS blockchain-based auto insurance sector. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 1-7). IEEE.
[10] Jin, S., Yao, X., Wang, S., & Wu, Y. (2021). Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS. Journal of Medical Systems, 45(5), 48.
[11] Choi, Nakhoon, and Heeyoul Kim. "A Blockchain-based user authentication model using MetaMask." Journal of Internet Computing and Services 20, no. 6 (2019): 119-127.
[12] Rahut, Shantanu Kumar, Razwan Ahmed Tanvir, Sharfi Rahman, and Shamim Akhter. "Scientific paper peer-reviewing system with blockchain, IPFS, and smart contract." In Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government, pp. 1029-1060. IGI Global, 2021.
[13] Basha, Shabeen A., Mohammed M. Elgammal, and Bana M. Abuzayed. "Online peer-to-peer lending: A review of the literature." Electronic Commerce Research and Applications 48 (2021): 101069.
[14] Daniel, Erik, and Florian Tschorsch. "IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks." IEEE Communications Surveys & Tutorials 24, no. 1 (2022): 31-52.
[15] Kumar, Randhir, and Rakesh Tripathi. "Building an ipfs and blockchain-based decentralized storage model for medical imaging." In Research Anthology on Improving Medical Imaging Techniques for Analysis and Intervention, pp. 916-934. IGI Global, 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

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