Advancing Cloud Ecosystems: The Role of Serverless Computing and Blockchain in Modern Infrastructure

S. Sivaranjani[1], K. Ramya[1] and R. Anandhi[2]
[1]*Department of Information Technology and BCA, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, Tamil Nadu, India*
[2]*Department of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai, Tamil Nadu, India*

Keywords: Cloud Computing, Serverless Computing, Blockchain Technology, Immutability, Cloud Security.

Abstract: In the digital age, cloud computing has transformed the way services are delivered by providing unparalleled cost-effectiveness, scalability, and agility. What is Serverless Computing An application of Cloud Computing, Serverless computing is distinct from its models in that it alleviates developers from the burden of infrastructure management so they can focus on the code. Key advantages of this strategy include lower costs, automated scalability, and faster time to market. To complement this development, blockchain technology that provides decentralized technical approaches to manage data, improves security, transparency, and trust. Combining Blockchain with Serverless Architectures Enable Organizations to Build Future-Ready Applications with Improved Operational Efficiency and Robust Security Capabilities This paper explores how these revolutionary technologies are converging and how they are likely to converge to build the next generation of applications.

SCITEPRESS
SCIENCE AND TECHNOLOGY PUBLICATIONS

1 INTRODUCTION

Cloud computing is a paradigm shift in the way computing resources are provisioned and consumed. It has transformed how organizations and people work by offering access to a pool of online resources, facilitating operations efficiencies. This technology alleviates users from the responsibility of maintaining infrastructure by allowing them to buy processing power, storage, and networking capabilities in the cloud when they are needed storage (Sina Ahmadi, 2024). As per National Institute of Standards and Technology (NIST), cloud computing is defined as "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. It becomes possible to rapidly provision and make available networks, servers, storage, applications and services with minimal administration overhead. As organizations turn increasingly to data-driven decision-making and request real-time access to services, cloud computing provides the environment needed to encourage innovation and responsiveness. Its capabilities fit various business scenarios — from deploying mobile apps to doing extensive data analytics.

1.1 Server Computing: Traditional Cloud

Dedicated servers or virtual machines are used to host apps and services in server computing, also known as conventional computing or server-based computing. For decades, this paradigm has been the norm for many organizations, and it depends on real or virtual servers to supply the resources required for data management, processing, and storage (Sina Ahmadi, 2024).

1.2 Limitations of Traditional Cloud Computing

Since every coin has two sides, cloud computing technology has also its own limitations as listed below:

Expensive: The requirement for a sizable initial hardware investment and continuing operating expenses can be very onerous.

Scalability issues: Increasing or decreasing involves a lot of preparation and technical know-how and is frequently not agile.

Sivaranjani, S., Ramya, K. and Anandhi, R.
Advancing Cloud Ecosystems: The Role of Serverless Computing and Blockchain in Modern Infrastructure.
DOI: 10.5220/0013869600004919
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 584-590
ISBN: 978-989-758-777-1
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

Underutilization of Resources: Inefficiencies may result from many servers not being used to their maximum potential.

Maintenance Overhead: Needs constant supervision and upkeep, which might use up important IT resources.

2 SERVERLESS COMPUTING: REVOLUTIONIZING CLOUD APPLICATIONS

Developers can create and execute applications using serverless computing without having to worry about maintaining servers. It mainly charges and scales automatically according to consumption. Event-driven architectures in serverless computing are bringing a major transformation to cloud applications environment (Y. Li et al., 2023). In a conventional cloud context, developers are often plagued by the challenges associated with provisioning and maintaining servers, which can slow them down and hike up operational costs. In serverless computing, however, this infrastructure management is abstracted, allowing developers to write functions that are automatically triggered by triggers such as user events, system events, or scheduled jobs (M. Ghobaei-Arani and M. Ghorbian, 2023).

2.1 The Evolution of Serverless Computing

Serverless computing is one of the most creative innovations in cloud computing. Serverless computing is a cloud computing execution model in which the cloud provider dynamically allocates machine resources.

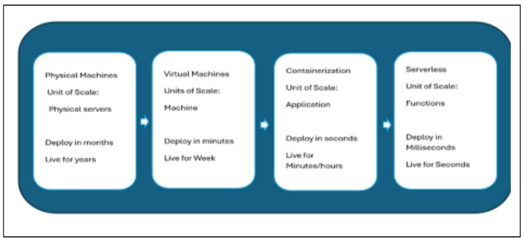

Figure 1: Evolution of Serverless Computing.

The provider takes care of server provisioning, scaling, and deployment while developers write and run the code (Mugunthan, S. R, 2021). This technique abstracted server maintenance, lets us focus on application functionality and logic is shown in Figure 1.

2.2 Event-Driven Workflow in Serverless Computing

Event-driven workflows of serverless computing provide a new methodology to build modern apps that respond rapidly and in real time to events without worrying about maintaining underlying infrastructure (Mugunthan et al., 2021). In a serverless architecture, developers create functions that respond to various triggers, such as user activities, system events or scheduled events, enabling seamless scaling and cost effectiveness.

Cloud providers offer their own solutions (e.g., AWS Lambda, Azure Functions), where applications can scale automatically based on the current demand. The paradigm also leads to challenges like vendor lock-in, difficulty in monitoring and debugging, and latency because of cold starts (Chen et al., 2021), thus careful design is important. Using serverless event driven processes has many benefits: scalability and cost effectiveness to name a few. Because they only pay for the precise amount of resources used during execution, companies can optimize resource utilization and lower costs associated with idle processing power by only executing code when an event happens.

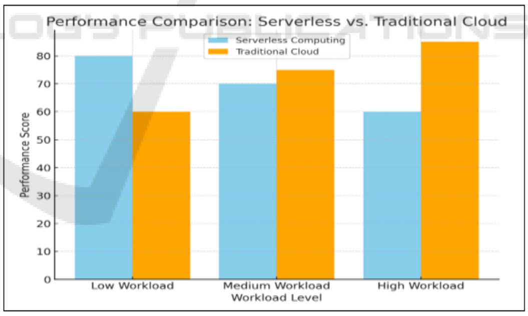

Figure 2: Performance of Serverless Computing Vs. Traditional Cloud Models.

Figure 2 demonstrates how serverless computing works with quick scalability and low latency and allows it to operate well at low workloads when compared to traditional cloud models. However, because they provide consistent resource allocation and circumvent serverless functions' cold start latency, traditional cloud models perform better than serverless at large workloads (Smys et al., 2021).

2.3 Benefits of Serverless Computing

There are many benefits of serverless computing greatly improving the creation of contemporary applications.

2.3.1 Cost Efficiency

Because serverless computing uses a pay-as-you-go pricing model, businesses only must pay for the computer resources they really utilize during runtime. This results in significant cost reductions by removing expenses related to idle resources (Srikanth et al., 2021).

2.3.2 Scalability

In response to demand, serverless architecture automatically scale resources up or down. Applications may manage different workloads thanks to their elastic scalability without the need for human intervention. Functions can automatically duplicate during periods of high traffic, guaranteeing steady performance in contrast, resources can be lowered appropriately during periods of low demand (Suma etb al., 2021).

2.3.3 Reduced Operational Overhead

Cloud service providers cover a large portion of the operational load associated with serverless computing, including server management and maintenance (Kumar et al., 2021). This enables development teams to devote more resources to innovation and application development as opposed to operational duties.

Figure 3 illustrates the cost efficiency of hosting the serverless computing and traditional cloud models based on execution time. The summary of the above graph is:

1. **Serverless Computing:**
   - Cost scales linearly with execution time.
   - Lower cost for short-duration tasks due to the pay-as-you-go model.
2. **Traditional Cloud:**
   - It has a higher baseline cost, even for short tasks.
   - More cost-effective for long-running workloads due to fixed pricing.

Hence, Serverless computing is ideal for short, bursty workloads, while traditional cloud suits long-running, predictable workloads (Jain et al., 2020).

Figure 3: Cost Efficiency in Serverless Computing Vs. Traditional Cloud Models.

2.4 Real-World Applications for Serverless Computing

Numerous real-world applications that make use of serverless computing's scalability, affordability, and simplicity of deployment have emerged because of its considerable popularity across a range of industries (Mugunthan, S. R, 2020).

- Companies like Netflix process enormous volumes of real-time data using serverless architecture, which helps them effectively manage customer demands and improve streaming quality.
- To handle erratic traffic during sales events, e-commerce systems like Zalando use serverless functions, which allow them to flexibly scale resources to match client demand without overprovisioning.
- To minimize operational costs and ensure responsiveness, service providers like Slack also use serverless solutions for background operations like data integration and notifications (Chen et al., 2024).
- In the financial sector, fintech firms use serverless computing to quickly process transactions as well as handle user authentication that requires high levels of security without compromising on efficiency.

3 IMPROVING CLOUD SECURITY USING BLOCKCHAIN

While cloud computing provides scalability, flexibility, and cost-efficiency, it also brings forth security challenges concerning data privacy, access control, and cyber threats. These risks need to be addressed by organizations to have secure cloud environments (V et al., 2020). The following are some major issues with cloud security:

1. **Data Loss & Breach**: As cloud providers store plenty of private data, they are often a victim of cyberattacks. Unauthorised access due to weak authentication or poor storage config can lead to data leaks
2. **Inadequate Identity and Access Management (IAM):** If authentication processes are not up to the mark, unauthorized users might access the cloud resources. Security issues may arise from poorly designed IAM roles with excessive permissions (Sha et al., 2020).
3. **Insecure Interfaces and APIs:** Cloud services use Application Programming Interfaces, or APIs, to communicate. Attackers can use vulnerabilities in badly configured APIs to gain unauthorized access Yadav et al., 2024).
4. **Cloud Settings Misconfiguration**: Misconfigured databases, storage buckets, and access controls can expose sensitive information. Such security breaches are common as most default settings are never changed.
5. **Insufficient Cloud Visibility and Monitoring**: Organizations have trouble monitoring cloud resources due to dynamic scaling and multi-cloud environments. In a scenario where there is insufficient visibility, unauthorized activities are nearly impossible to detect.
6. **Compliance and Legal Issues:** The data protection laws vary in different countries (GDPR, HIPAA, CCPA). Companies using cloud services must protect data in accordance with these regulations.
7. **Insider Threats (Negligent Employees)**: Employees/insider with privileged access can help in violating cloud resources Sensitive information can be exposed due to accidental data deletion or phishing attacks.

3.1 Understanding Blockchain Technology

Blockchain technology is one of the most revolutionary inventions that can change lives in all sectors. Blockchain is a shared, decentralized ledger system that allows secure and open transactions to be conducted without intermediaries. Blockchain is a distributed digital ledger that securely records transactions on many computers (Gupta et al., 2024). Unlike traditional centralized systems, this system operates on a distributed network, which makes it impervious to fraud and tampering. Transactions are collected in blocks, which are linked together to create a chain, hence the term "blockchain". It has some features such as immutability, which means transaction which is once recorded can never be altered or deleted, which ensures security and trust. With respect to validation of transactions, it replaces the need for intermediaries using consensus mechanisms (Gupta et al., 2024).

Structure of Blockchain

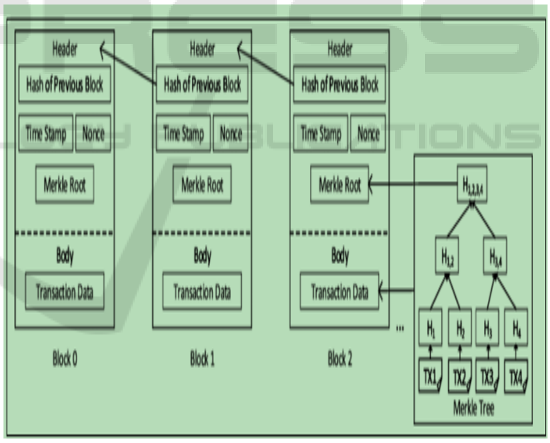

Figure 4: Structure of Blockchain.

Figure 4 shows the architecture of Blockchain. It consists of blocks, each containing a set of transactions, a timestamp, and a cryptographic hash linking it to the previous block, forming an immutable chain (Patel et al., 2023). The key components of blockchain include nodes (participants in the network), consensus mechanisms (such as Proof of Work or Proof of Stake), smart contracts, and cryptographic security. Blockchain operates without a central authority by relying on **consensus**

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

mechanisms for transaction validation. Common mechanisms include,

- **Proof of Work (PoW)** - Miners solve cryptographic puzzles to validate transactions (e.g., Bitcoin).
- **Proof of Stake (PoS)** - Validators are chosen based on the number of coins they hold (e.g., Ethereum 2.0).

3.2 How Blockchain Improves Cloud Security

Blockchain technology offers numerous benefits across various industries by enhancing security, transparency, efficiency, and decentralization (Rajasekar, P et al., 2024). One of its key advantages is improved security, as blockchain uses cryptographic encryption and decentralization to prevent fraud, hacking, and data manipulation. Additionally, it ensures immutability, meaning once a transaction is recorded, it cannot be altered or deleted, making data tamper-proof (Liu et al., 2020).

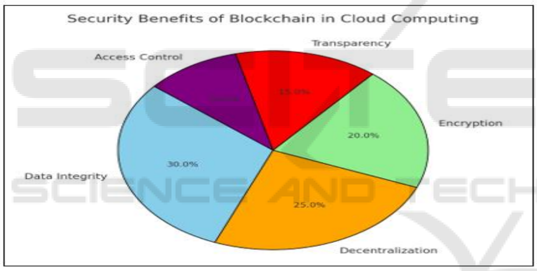

Figure 5: Security Benefits of Blockchain in Cloud Computing.

Figure 5 shows the security advantages of blockchain in cloud computing are highlighted in the pie graph. Decentralization (25%) lessens dependency on central authority, while data integrity (30%) guarantees tamper-proof records. Transparency (15%) increases confidence by permitting verifiable records, while encryption (20%) safeguards sensitive data. 10% access control prevents unwanted access. Integrity, decentralization, encryption, transparency, and access control are some of the ways that blockchain improves cloud security overall.

3.3 Performance Comparison

Cloud security has been improved by incorporating Blockchain through its immutability feature. There are evident advantages in implementing blockchain in cloud model rather than cloud model without blockchain. Table 1 gives the performance comparison of systems with blockchain vs. without blockchain across key factors like security, transparency, decentralization, speed, cost, scalability, trust and automation.

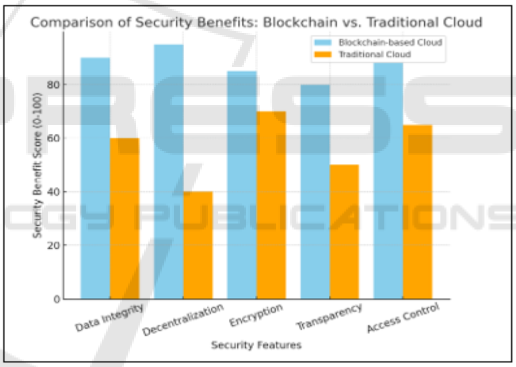

Figure 6: Comparison of Benefits of Blockchain Vs Traditional Cloud.

Table 1: Cloud Model With Vs. Without Blockchain.

Factor	Cloud with Blockchain	Cloud without Blockchain
Security	High security due to cryptographic encryption and immutability.	Vulnerable to hacking, fraud, and data tampering.
Transparency	Transactions are recorded on a public or permissioned ledger, ensuring transparency.	Limited transparency, data can be hidden or manipulated.
Decentralization	Operates on a distributed network with no central authority.	Centralized control, prone to single points of failure.
Speed	It can be slower due to consensus mechanisms and network validation.	Faster in centralized systems with direct processing.
Cost	Reduces intermediary costs but may have higher computational expenses.	Lower computational costs but may require intermediaries.
Scalability	Limited scalability, especially for public blockchains like Bitcoin and Ethereum.	Easily scalable in traditional centralized systems.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Trust & Reliability	Trustless system where transactions are verified by the network.	Requires trust in a central authority or third parties.
Automation	Supports smart contracts for self-executing transactions.	Manual intervention often required for contract execution.

Figure 6 shows the security benefits of blockchain-based cloud and traditional cloud across five key factors: data integrity, decentralization, encryption, transparency, and access control (Liu et al., 2020).

The blockchain-based cloud (blue bars) consistently scores higher in all aspects, particularly in decentralization and transparency, where the traditional cloud (orange bars) lags. Encryption and access control also show significant improvements in blockchain-based solutions (Habib et al., 2025). Overall, the chart highlights blockchain's superior security benefits over traditional cloud computing, making it a more secure and reliable choice for data protection and management.

4 CONCLUSIONS

This article hence brings out the improvement of cloud infrastructure using serverless computing and blockchain technology (Modi, R et al., 2024). Table 2 shows the comparison of serverless computing and cloud models with Blockchain based upon the metrics like security architecture, data integrity, authentication, attack resistance, compliance, performance and cost implications.

Table 2: Serverless Computing Vs. Cloud With Blockchain.

Factor	Serverless Computing	Cloud with Blockchain
Security Architecture	Relies on cloud providers to manage security, including infrastructure, runtime, and application security.	Uses decentralized security mechanisms, cryptographic hashing, and consensus protocols to ensure data integrity and immutability.
Data Integrity and Confidentiality	Data is processed and stored in a centralized cloud environment, making it vulnerable to data breaches and insider threats.	Provides tamper-proof records with cryptographic security, making it more resilient to unauthorized modifications.
Authentication and Access Control	Implements identity and access management (IAM) controls, role-based access, and API gateways for authentication.	Uses cryptographic keys and decentralized identity management, reducing dependency on traditional centralized authentication mechanisms.
Attack Resistance	Prone to Distributed Denial-of-Service (DDoS) attacks, dependency vulnerabilities, and supply chain risks.	More resistant to DDoS and single-point failures due to decentralization but may face Sybil and 51% attacks in public networks.
Compliance and Privacy	Compliance depends on the cloud provider's adherence to regulations (GDPR, HIPAA, etc.), with limited user control.	Offers enhanced transparency and auditability, but privacy can be challenging in public blockchains.
Performance and Scalability	Highly scalable with dynamic resource allocation but may suffer from cold start delays.	Scalability issues in public networks due to consensus mechanisms, leading to slower transaction processing.
Cost Implications	Pay-as-you-go model reduces infrastructure costs but may lead to unpredictable expenses.	Higher computational and storage costs, especially in proof-of-work-based systems.

Therefore, serverless computing is ideal for scalable cloud applications but requires robust security management. Blockchain provides enhanced data integrity and decentralization but faces performance and privacy challenges (Raghu et al., 2025).

REFERENCES

Chen, Joy Iong-Zong, and Lu-Tsou Yeh, "Greenhouse Protection Against Frost Conditions in Smart Farming using IoT Enabled Artificial Neural Networks." Journal of Electronics 2, no. 04 (2020): 228-232.

Chen, Joy Iong Zong, and Joy Iong Zong. "Automatic Vehicle License Plate Detection using K-Means Clustering Algorithm and CNN." Journal of Electrical Engineering and Automation 3, no. 1: 15-23, 2021.

Gupta, Harshita, and Prabhat Verma. "A survey on data security and latency Frameworks in healthcare using Blockchain." In 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1745-1750. IEEE, 2024.

Habib, Gousia, Sparsh Sharma, Sara Ibrahim, Imtiaz Ahmad, Shaima Qureshi, and Malik Ishfaq. "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing." Future Internet 14, no. 11 (2022): 341.

Hengjinda, P., Dr Chen, and Joy Iong Zong. "An Intelligent Feedback Controller Design for Energy Efficient Air Conditioning System." Journal of Electronics and Informatics 2, no. 3: 168-174, 2020.

Hussein, K., & Al-Gailani, M. (2022). An Efficient Bandwidth Based on the Cryptographic Technique of the RSA Accumulator in Block Chain Networks. 2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT), 164-168.

Jain, Sukrutha A., and Avinash Bharadwaj, "Characterizing WDT subsystem of a Wi-Fi controller in an Automobile based on MIPS32 CPU platform across PVT." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 04: 187- 196, 2020.

Kumar, T. Senthil. "Study of Retail Applications with Virtual and Augmented Reality Technologies." Journal of Innovative Image Processing (JIIP) 3, no. 02 144-156, 2021.

Liu, Haibing, Rubén González Crespo, and Oscar Sanjuán Martínez. "Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts." In Healthcare, vol. 8, no. 3, p. 243. MDPI, 2020.

M. Ghobaei-Arani and M. Ghorbian, "Scheduling Mechanisms in Serverless Computing" in Serverless Computing: Principles and Paradigms, Cham: Springer International Publishing, pp. 243-273, 2023.

Modi, R., Jammoria, A. S., Pattiwar, A., Agrawal, A., & Raja, S. P. (2025). Secure system to secure crime data using hybrid: RSA- AES and hybrid: Blowfish-Triple DES. International Journal of Electronic Security and Digital Forensics, 17(1-2), 194-232.

Mugunthan, S. R, "Decision Tree Based Interference Recognition for Fog Enabled IOT Architecture." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 01: 15-25, 2020.

Mugunthan, S. R., "Wireless Rechargeable Sensor Network Fault Modeling and Stability Analysis." Journal of Soft Computing Paradigm (JSCP) 3, no. 01: 47-54,2021.

Mugunthan, S. R., and T. Vijayakumar. "Design of Improved Version of Sigmoidal Function with Biases for Classification Task in ELM Domain." Journal of Soft Computing Paradigm (JSCP) 3, no. 02 :70-82,2021.

Patel, Rahul K., Deekshitha Somanahalli Umesh, and Nikunj R. Patel. "Improving Cloud Security Using Distributed Ledger Technology." In Privacy Preservation and Secured Data Storage in Cloud Computing, pp. 135-153. IGI Global, 2023.

Raghu, N., Bhat, R., Nambiar, P. R., Shetty, G. S., & DB, A. K. (2025). Blockchain-Enhanced GAN Image Encryption Scheme for Cloud Computing. In Intellige nt Systems and IoT Applications in Clinical Health (pp. 367-392). IGI Global.

Rajasekar, P., K. Kalaiselvi, Raju Shanmugam, S. Tamilselvan, and A. Pasumpon Pandian. "Advancing Cloud Security Frameworks Implementing Distributed Ledger Technology for Robust Data Protection and Decentralized Security Management in Cloud Computing Environments." In 2024 Second International Conference on Advances in Information Technology (ICAIT), vol. 1, pp. 1-6. IEEE, 2024.

Sha, Srirang K., and Shweta Jha,"An Integrated Model of Sustainable Management Systems for Start-ups." In International Conference on Mobile Computing and Sustainable Informatics, pp. 337-342. Springer, Cham, 2020.

Sina Ahmadi, "Challenges and solutions in network security for serverless computing", Int. J. Curr. Sci. Res. Rev. 7, 01 (2024), 218–229, 2024

Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain- based Architectural Framework." Journal of Artificial Intelligence 3, no. 02: 90-100,2021.

Srikanth, M. S., TG Keerthan Kumar, and Vivek Sharma. "Automatic Vehicle Service Monitoring and Tracking System Using IoT and Machine Learning." In Computer Networks, Big Data and IoT, pp. 953-967. Springer, Singapore, 2021.

Suma, V. "Community Based Network Reconstruction for an Evolutionary Algorithm Framework." Journal of Artificial Intelligence 3, no. 01 :53-61, 2021.

ty management scheme of cloud storage based on blockchain and digital twins. J Cloud Comp 13, 15 (2024). https://doi.org/10.1186/s13677-023-00587-4

Y. Li, Y. Lin, Y. Wang, K. Ye and C.-Z. Xu, "Serverless computing: State-of-the-art challenges and opportunities", IEEE Trans. Serverless Computing., vol. 16, no. 2, pp. 1522-1539, Mar./Apr. 2023.

Yadav, Dhananjay, Aditi Shinde, Akash Nair, Yamini Patil, and Sneha Kanchan. "Enhancing data security in cloud using blockchain." In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 753-757. IEEE, 2020.