WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BLOCKCHAIN BASED DECENTRALISED STORAGE DESIGN FOR DATA CONFIDENCE OVER CLOUD NATIVE EDGE INFRASTRUCTURE

P.LOGIAYAN[1] MANDA DIVYA DURGA[2]

[1]Professor, Department of MCA, Sri Manakula Vinayagar Engineering College-605107,India.
PG Student, Sri Manakula Vinayagar Engineering College-605107,India
Logaiyan.mca@smavec.ac.in[1] divyamanda1508@gmail.com[2]

ABSTRACT:

As the modern computing market experiences a surge in demand for efficient data-management solutions, challenges posed by centralized storage systems become more pronounced, especially with the proliferation of Internet of Things devices. Centralized storage, although cost-effective, faces issues of scalability, performance bottlenecks, and security vulnerabilities. With decentralized storage, data are distributed across nodes, offering redundancy, data availability, and enhanced security. Unfortunately, decentralized storage introduces its own challenges, such as complex data retrieval processes, potential inconsistencies in data versions, and difficulties in ensuring data privacy and integrity in a distributed setup.

Keywords: - Key concepts include *decentralized and centralized storage***,** *data management*, and the impact of *IoT* on storage demands. Keywords also cover *scalability*, *security***,** *data availability***,** *privacy*, and *distributed systems*.

INTRODUCTION:

In the digital age, healthcare systems are rapidly evolving with the integration of smart technologies such as IoT (Internet of Things) and cloud computing. Remote Health Monitoring Systems (RHMS) allow patients to share health data with healthcare providers through wearable sensors and mobile apps, enabling real-time monitoring and faster medical interventions. However, as these systems handle sensitive personal data, data security and integrity are major concerns—particularly threats posed by malicious insiders such as administrators with privileged access. This project addresses these security challenges by implementing a blockchain-based logging system integrated with a Cloud Access Security Broker (CASB). The goal is to prevent tampering of log data and enhance the traceability of data access events, thereby boosting trust and transparency in health data management systems

Project Objectives:

- To develop a secure and auditable logging mechanism for remote health monitoring data.
- To track all actions (e.g., viewing, uploading, modifying) performed on patient data in real time.
- To store log records in an immutable private blockchain, preventing tampering or deletion.
- To allow patients and auditors to view log history and detect suspicious activity.
- To integrate with a CASB module that enforces fine-grained access control using encryption policies.

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating System and Language can be used for developing the tool. The literature from 2019 to 2024 highlights significant advancements in credit card fraud detection for web applications. Machine learning and AI, combined with behavioral biometrics and blockchain, are transforming mobile security. However, challenges remain in balancing security and usability, managing resource constraints, and ensuring data privacy. Emerging technologies like federated learning, quantum cryptography, and explainable AI hold promise for future development

1) Object storage in the cloud and multi-cloud: State of the art and the research challenges AUTHORS: V. Bucur, C. Dehelean, and L. Miclea The cloud has been one of the hottest topics of discussion in the information technology field, both in terms of research and on a commercial level, since its inception in the late 2000s. The ever increasing need for better, faster and more powerful computers to process the ever increasing amount of data has made the

cloud an indispensable feature of modern IT. Due to its massive storage power the cloud has allowed corporate users, private users and researchers to centralize all their data and have access to it almost constantly so long as they have an internet connection.

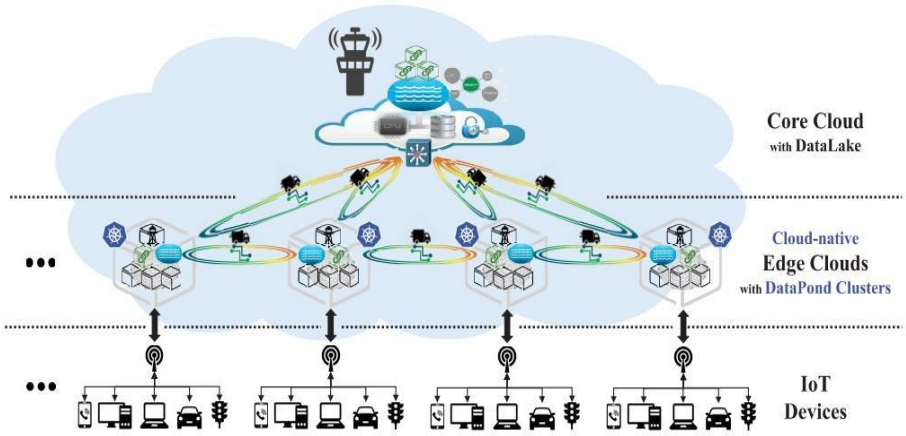
2) Ananke: A framework for cloud-native applications smart orchestration AUTHORS: A. Di Stefano, A. Di Stefano, and G. Morana Micro-service architecture enables smarter management of applications life-cycle. However, the increasing of the number of components also increases complexity, especially on operations like migration and horizontal scaling. While operations, in monolithic systems, involve only one component, operations in micro-services based applications can get complex and should involve parameters and properties like connection throughput, resources usage, robustness or consistency and reliability.

3) Meta-key: A secure data-sharing protocol under blockchain-based decentralized storage architecture AUTHORS: D. Li, R. Du, Y. Fu, and M. H. Au In this project i propose Meta-key, a data-sharing mechanism that enables users share their encrypted data under a blockchain-based decentralized storage architecture. All the dataencryption keys are encrypted by the owner's public key and put onto the blockchain for safe and secure storage and easy key-management. Encrypted data are stored in dedicated storage nodes and proxy re-encryption mechanism is used to ensure secure data-sharing in the untrusted environment.

PROPOSED SYSTEM:

The proposed system is a Blockchain-Based Decentralized Storage Design that integrates cloud-native principles to ensure data confidence, scalability, and security over a distributed edge infrastructure. This architecture is specifically designed to overcome the limitations of centralized and traditional decentralized storage systems by combining the strengths of blockchain technology with the flexibility of cloud-native orchestration. In this system, data is stored across multiple nodes—referred to as Data Pond Nodes—within an edge cloud environment. These nodes work in coordination with Management Nodes that handle container orchestration, resource allocation, and workload balancing using cloud-native tools. Additionally, Data Transfer Nodes are employed to facilitate secure and efficient data transfer between different storage clusters.

IMPLEMENTATION:



The architectural design of the system illustrates the high-level structure and communication flow between various components involved in a real-time chat and calling application. It ensures that the system is modular, scalable, and supports real- time data transmission

The implementation of this project begins at the IoT device layer, where various sensors and connected devices such as traffic lights, vehicles, and smart meters are deployed to continuously generate real-time data. These devices are connected through wireless communication technologies like 5G or Wi-Fi, enabling seamless data transmission to the next layer. Lightweight client applications on these devices perform basic preprocessing such as filtering and formatting before sending data to the edge.

At the next level, cloud-native *Edge Clouds* are established close to the data sources using containerized infrastructure orchestrated by platforms like Kubernetes. These edge clouds host *DataPond Clusters*, which are responsible for processing, analyzing, and temporarily storing data locally. This reduces the dependency on centralized servers, lowers latency, and ensures quicker decision-making. Data is filtered, aggregated, and only relevant insights are forwarded to the core cloud, minimizing bandwidth usage.

The *Core Cloud* acts as a centralized data hub equipped with a *DataLake* for long-term storage, analytics, and machine learning model training. It receives refined data from multiple edge clouds, stores it efficiently using scalable storage solutions, and performs high-level analytics for business intelligence. This core layer ensures data consistency, redundancy, and archival across the system.

For secure and efficient data flow between IoT devices, edge clouds, and the core cloud, encrypted communication protocols are implemented, along with strict authentication and access control policies. Monitoring tools such as Prometheus and Grafana are used to track the performance and health of all layers in real time. The entire system is tested using synthetic workloads to evaluate its scalability, fault tolerance, and responsiveness, and is then optimized based on performance metrics to ensure a robust and efficient decentralized data management framework.

CONCLUSION:

This project introduces a decentralized storage system that integrates the strengths of blockchain technology and cloudnative concepts. With blockchain, we enhance data sharing security and transparent data validation. Meanwhile, cloudnative concepts such as containerization and orchestration improve the system's scalability and flexibility. We evaluate the performance on a high-end edge computing infrastructure and show that the proposed system consistently outperforms IPFS in terms of data transfer speed.

FUTURE ENHANCEMENT:

Future enhancements for the blockchain-based decentralized storage system can focus on improving scalability, security, and usability through the integration of advanced technologies. One significant direction is adopting more efficient consensus algorithms such as Proof of Stake or Practical Byzantine Fault Tolerance, which can reduce latency and energy consumption compared to traditional methods. Incorporating artificial intelligence and machine learning at both edge and cloud layers can enable predictive analytics, anomaly detection, and intelligent resource management, thereby enhancing system responsiveness and security.

REFERENCES:

[1] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, ''State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions,'' Sustainability, vol. 13, no. 16, p. 9463, Aug. 2021.

[2] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, ''A survey on proof of retrievability for cloud data integrity and availability: Cloud storage stateof-the-art, issues, solutions and future trends,'' J. Netw. Comput. Appl., vol. 110, pp. 75–86, May 2018.

[3] M. Factor, K. Meth, D. Naor, O. Rodeh, and J. Satran, ''Object storage: The future building block for storage systems a position paper,'' in Proc. IEEE Int. Symp. Mass Storage Syst. Technol., Aug. 2005, pp. 119–123.

[4] D. Guide, ''Amazon simple storage service,'' Tech. Rep., 2008.

[5] V. Bucur, C. Dehelean, and L. Miclea, ''Object storage in the cloud and multi-cloud: State of the art and the research challenges,'' in Proc. IEEE Int. Conf. Autom., Quality Test., Robot. (AQTR), May 2018, pp. 1–6.

[6] J. Kosińska and K. Zieliński, ''Autonomic management framework for cloud-native applications,'' J. Grid Comput., vol. 18, no. 4, pp. 779–796, Dec. 2020.