HYBRID CLOUD DATABASE FRAMEWORK FOR MODERNIZING LEGACY DATA SYSTEMS

N. Siva Kumar
Research Scholar
University of Technology
Jaipur.

Dr. Suneel Pappala
Research Supervisor
University of Technology
Jaipur.

Dr. Rama Sree
Research Co-Supervisor
University of Technology
Jaipur.

ABSTRACT

Modernizing legacy systems is critical for organizations striving to enhance operational efficiency, scalability, and security in an increasingly data-driven and digital landscape. Traditional infrastructures, burdened by technical debt, security vulnerabilities, and operational inefficiencies, pose significant challenges to innovation and long-term sustainability. This paper explores a scalable approach to legacy system modernization, emphasizing next-generation data architectures and seamless integration strategies. It examines the limitations of outdated systems, the benefits of cloud-native and distributed architectures, and the role of micro services and event-driven frameworks in improving system agility It also discusses data integration strategies, compares ETL and ELT processes, and highlights the significance of middleware solutions, API-driven ecosystems, and hybrid cloud environments in ensuring interoperability. The paper concludes with recommendations for organizations seeking to transform legacy systems, advocating for structured modernization roadmaps, security-centric designs, and future-proof architectural strategies. The modernization of legacy systems through migration to cloud-based platforms has become a cornerstone of enterprise IT transformation. In particular, the transition of Unix-based infrastructures long regarded as the foundation of mission-critical operations into hybrid cloud environments underscores the growing need for scalability, agility, and operational efficiency. Architecting hybrid Unix environments involves harmonizing the reliability and proven capabilities of Unix with the dynamic features of cloud computing.

Keywords: *Legacy System Modernization, Scalable Data Architectures, Hybrid Cloud Environments, Data Migration Strategies*

INTRODUCTION

This is where databases come into the picture. A database is a structured collection of data that is organized, stored, and managed to enable easy retrieval, manipulation, and analysis. It serves as a centralized repository for storing and accessing large volumes of structured and unstructured data. Databases provide a structured framework for organizing data, ensuring data integrity, and facilitating efficient data processing. Over the years, databases have evolved significantly, driven by advancements in technology and changing data management needs. Traditional relational databases have been the foundation of data management for several decades, offering a structured approach with tables, rows, and columns. In the cloud computing model, a wide chain of systems is interconnected in private and public networks to provide complex, flexible, and secure information, data, and storage resources. With this technology's breakthrough in computer resource prices, web hosting and remote networking are reducing massive sums. Cloud-enabled applications are realistic ways to achieve immediate cost savings rather than investing significant money on building up a new IT system. One of the strengths is cost dependent as per necessity. Cloud computing helps organizations to solve the related problems by reducing costs, better performance and fast IT service responses. However, many organizations concern on the security of cloud computing systems because of storing important information on

someone else storage. Securing information data in cloud systems can be an important issue because of cloud systems is a collection of many system and cannot be managed by specific data and software owners. We thought to develop a private database cloud system instead of classic cloud systems. There are many security solutions for private database clouds. While databases are under these types of attacks, some precautions must be taken in order to provide database security. Legacy system modernization has emerged as a critical priority for organizations aiming to remain competitive in the rapidly evolving digital landscape. Organizations that fail to transition toward next-generation architectures risk falling behind competitors that embrace digital transformation. Modernizing legacy systems enables enterprises to optimize workflows, improve user experiences, and drive operational efficiency. It also allows businesses to integrate advanced analytics, automation, and cloud-based solutions, providing a foundation for long-term growth and adaptability

LITERATURE REVIEW

J. Shahithya (2023) This study explores the concept of cloud database, which leverages the power of cloud computing to provide scalable and flexible data management solutions. It discusses the benefits, challenges, and considerations associated with adopting cloud databases, along with various architectural models and deployment options. The chapter also delves into the key features, such as elasticity, high availability, and data security, offered by cloud databases. Furthermore, it examines the role of cloud databases in modern applications, including their integration with other cloud services and their ability to support big data analytics. The chapter concludes by highlighting future trends and advancements in cloud database technologies.

Satish S R V Karuturi (2023) The majority of enterprises have recently enthusiastically embraced cloud computing, and at the same time, the database has moved to the cloud. This cloud database paradigm can lower data administration expenses and free up new business to concentrate on the product that is being delivered. Furthermore, issues with scalability, flexibility, performance, availability, and affordability can be resolved with cloud computing. Security, however, has been noted as posing a serious risk to cloud databases and has been essential in fostering public acceptance of cloud computing. Several security factors should be taken into account before implementing any cloud database management system. These features comprise, but are not restricted to, data privacy, data isolation, data availability, data integrity, confidentiality, and defense against insider threats. In this paper, we discuss the most recent research that took into account the security risks and problems associated with adopting cloud databases. In order to better comprehend these problems and how they affect cloud databases, we also provide a conceptual model.

Norah Farooqi (2022) Cloud computing paved the way to many technical facilities for companies to develop their business needs in more effective and efficient manner. Combining private and public cloud into so called Hybrid cloud has made a positive leap in business by allowing applications and data to be shared among enterprises. However, many challenges and issues have arisen when adopting the hybrid

cloud to manage, store and process data. The most critical one of these challenges is the security of the adopted Hybrid cloud. This research presented a comprehensive study about the security challenges in the Hybrid cloud computing as well as the suggested solutions. The study used a Systematic Literature Review (SLR) process to collect, review and summarize published articles from IEEE and Springer Nature databases and between 2020 and 2021. As a result, there were 7 eligible articles selected according to the search criteria and fully reviewed. The findings have revealed that there are four main challenges which are Data Security, Access Control, Privacy, Data Leakage and Cy- ber Attacks. Future studies should be conducted using different databases to have further investigation regarding the security in Hybrid clouds.

Zayaraz G. (2021) In this study an efficient lightweight cloud-based data security model (LCDS) is proposed for building a secured cloud database with the assistance of intelligent rules, data storage, information collection, and security techniques. The major intention of this study is to introduce a new encryption algorithm to secure intellectual data, proposing a new data aggregation algorithm for effective data storage and improved security, developing an intelligent data merging algorithm for accessing encrypted and original datasets. The major benefit of the proposed model is that it is fast in the encryption process at the time of data storage and reduced decryption time during data retrieval. In this work, the authors proposed an enhanced version of the hybrid crypto algorithm (HCA) for cloud data access and storage. The proposed system provides secured storage for storing data within the cloud.

Song Wang (2020) Database system is a very important information infrastructure of modern society. The consistent sharing of data is the key to the realization of reliable application of database system in different fields of society. With respect to the problems of data inconsistency that are widely existed in database system applications, we focus on the entity-relation modeling, the origin of data generation, combine with practical application cases and propose active and effective prior precautions which are extracted from our many years of teachings and scientific researches. First, we use the objective uniqueness of recognizing entity and relation to overcome the subjective biases in data modeling fundamentally. Next, some empirical rules for optimizing the entity-relation model are employed to further rectify the inappropriateness in the model. The effectiveness and feasibility of the proposed principles of the entity-relation modeling optimization for database system are sufficiently approved by the demon-stration of practical application cases.

Hybrid Cloud Database Architectures

Hybrid cloud database architecture merges features from public and private clouds, offering a versatile and scalable approach for database management. This enables organizations to leverage the scalability and cost efficiency of public clouds, while retaining control over sensitive data and applications in a private cloud environment. In hybrid cloud database architecture, data can be stored and processed in either public or private clouds, based on the specific requirements of the organization. For instance, sensitive data can be stored securely in a private cloud, while less sensitive data can be stored in a public cloud to achieve enhanced scalability and

cost efficiency. Hybrid cloud database architectures can easily scale up or down to meet changing demand, without the need for users to purchase and maintain expensive hardware. Hybrid cloud database architectures allow for more flexible allocation of resources, as data can be stored and processed in both public and private clouds depending on the specific needs of the organization.

Problems posed by legacy computing

Legacy systems are considered to be potentially problematic by some software engineers for several reasons. If legacy software runs on only antiquated hardware, the cost of maintaining the system may eventually outweigh the cost of replacing both the software and hardware unless some form of emulation or backward compatibility allows the software to run on new hardware. These systems can be hard to maintain, improve, and expand because there is a general lack of understanding of the system; the staff who were experts on it have retired or forgotten what they knew about it, and staff who entered the field after it became "legacy" never learned about it in the first place. This can be worsened by lack or loss of documentation. Comair Airline Company fired its CEO in 2004 due to the failure of an antiquated legacy crew scheduling system that ran into a limitation not known to anyone in the company. Legacy systems may have vulnerabilities in older operating systems or applications due to lack of security patches being available or applied. There can also be production configurations that cause security problems.

Migration models, approaches and frameworks

Moving on from strategies to a level of greater detail a variety of migration models, approaches and frameworks can be identified in literature. This work contributes to the actual solutions in the course of solving migration challenges. In REMICS approach the source architecture is migrated into cloud-capable target architecture by applying SOA and cloud computing patterns, replacing and wrapping legacy software components, and designing in a way that service composition is emphasized. Migration phase is supported by two additional concepts: Model-Driven Interoperability (MDI) which ensures that existing services can still interoperate with the services in the target architecture, and Validate, Control and Supervise activity which e.g. validates the target architecture against Quality of Service (QoS) requirements and test cases. Pre-migration consists of legacy software analysis and goal setting. In migration step the legacy software is reverse engineered into a model, which again is transformed into a higher level platform-independent model and further to a cloud-compatible model.

Additional uses of the term Legacy in computing

The term legacy support is often used in conjunction with legacy systems. The term may refer to a feature of modern software. For example, Operating systems with "legacy support" can detect and use older hardware. The term may also be used to refer to a business function; e.g. a software or hardware vendor that is supporting, or providing software maintenance, for older products. A "legacy" product may be a product that is no longer sold, has lost substantial market share, or is a version of a product that is not current. A legacy product may have some advantage over a modern product making it appealing for customers to keep it around. A product is only truly "obsolete" if it has an advantage to

nobody—if no person making a rational decision would choose to acquire it new. The term "legacy mode" often refers specifically to backward compatibility. A software product that is capable of performing as though it were a previous version of itself is said to be "running in legacy mode". This kind of feature is common in operating systems and internet browsers, where many applications depend on these underlying components.

Integration with Cloud Services

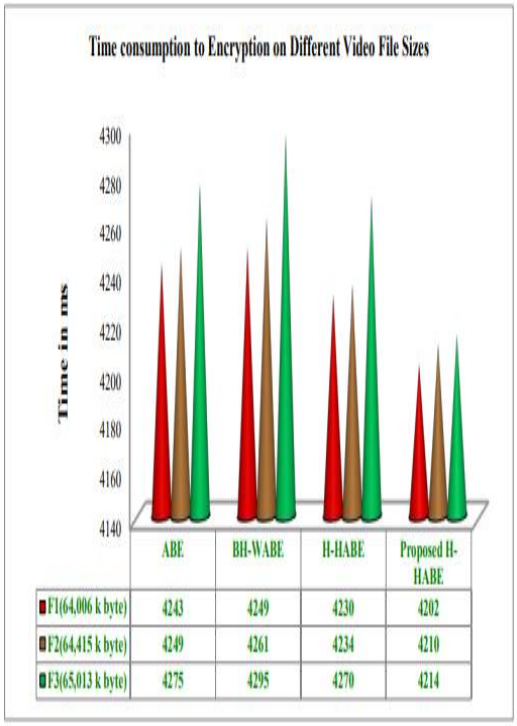
Integration with cloud services is a key advantage of using cloud databases in modern applications. Cloud databases can seamlessly integrate with a wide range of cloud services, enabling organizations to enhance their applications with additional functionalities and capabilities. Here are some common cloud services that can be integrated with cloud databases: Cloud databases can integrate with cloud storage services, such as Amazon S3, Google Cloud Storage, or Azure Blob Storage. This integration allows organizations to store large binary objects, multimedia files, backups, and other unstructured data outside of the database, leveraging the scalability and durability of cloud storage.

METHODOLOGY

The proposed access control method using H-HABE is designed to be utilized within a hierarchical multiuser data-shared environment, which is extremely suitable for a mobile cloud computing model to protect the data privacy and defend unauthorized or illegal access. Compared with the original HABE scheme, the new scheme can be more adaptive technique for mobile cloud computing environment to process, store and access the huge data and files while our new system can let different privilege entities access their permitted data and files. Our new scheme not only accomplishes the hierarchical access control of mobile sensing data in the cloud computing model, but protects the data from being obtained by an entrusted third party. In cloud computing, a secure and efficient data collaboration is achieved by the proposed hybrid H-HABE approach. Most of the conventional ABE methods only have a single authority to handle both the secret and public keys. However, in many circumstances, the consumers hold attributes from multi authority, and the data holders share data with consumers who are managed by a distinct authority. Many different multi authority attribute-based access control structures have been developed to solve this problem. In access control systems with the intention of updating the cipher text, a data holder has presented online for all time, besides the attributes that are given similar status. In the proposed scheme, the weighing of attributes is given by the AES and blowfish algorithm to provide secure data in cloud computing.

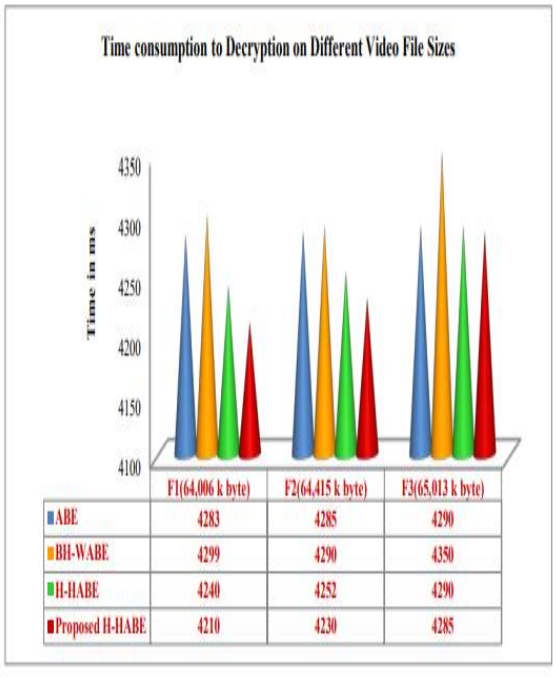
RESULTS AND DISCUSSIONS

Now here it makes a comparison between other types of data (Video files) to check which one can perform better in this case. Experimental results for video files in the format (.mp4) are shown in Graph 1 at encryption.



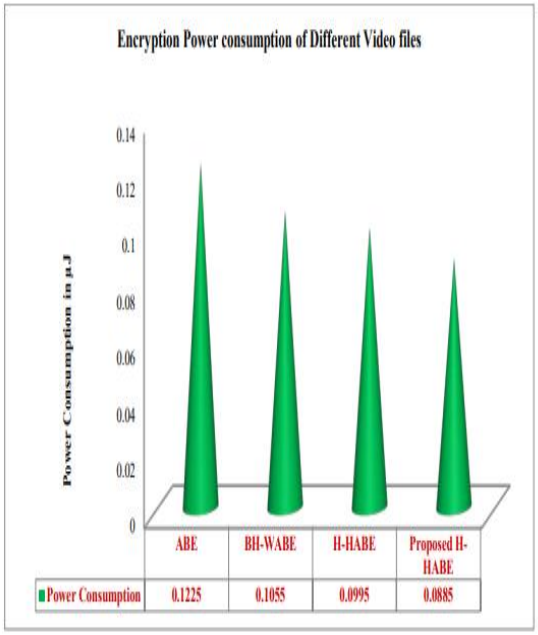
Graph.1 Encryption time with different sizes for video files

Now here it makes a comparison between other types of data (Video files) to check which one can perform better in this case. Experimental results for video files in the format (.mp4) are shown in Graph. 2 at decryption.



Graph. 2 Time consumption to Decryption on Different Video File Sizes

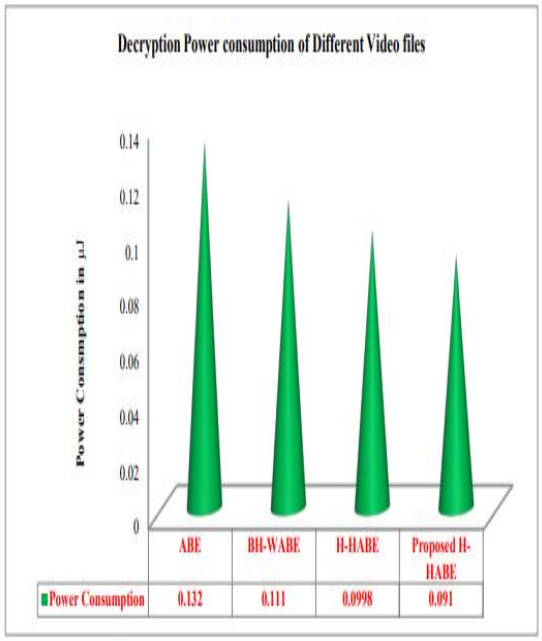
Graph. 3 shows the performance of cryptographic algorithms in terms of power consumption for encryption process with a different video file sizes.



Graph. 3 Encryption Power consumption of Different Video files

From those results, it is easy to observe that ABE still has disadvantage in encryption process over other algorithms in terms of time consumption and serially in throughput and power consumption. On the other hand, it is easy to observe that BH-WABE has disadvantage in encryption process over other algorithms in terms of time consumption and serially in throughput and power consumption.

Graph.4 shows the performance of cryptographic algorithms in terms of power consumption for decryption process with a different Video file sizes.



Graph. 4 Decryption Power consumption of Different Video files

From those results, it is easy to observe that ABE still has disadvantage in decryption process over other algorithms in terms of time consumption and serially in throughput and power consumption. On the other hand, it is easy to observe that BH-WABE has disadvantage in decryption process over other algorithms in terms of time consumption and serially in throughput and power consumption.

CONCLUSION

The transition from legacy database systems to hybrid cloud database architectures has become not only a technological imperative but also a strategic necessity for modern organizations. This study proposed a comprehensive framework designed to guide enterprises through the complexities of migrating traditional, tightly coupled, on-premises databases toward a flexible, scalable, and resilient hybrid cloud environment. The framework integrates technical, organizational, and operational considerations to ensure that legacy assets are modernized responsibly while leveraging the advantages enabled by cloud platforms. The findings of this work reaffirm that legacy systems, despite their robustness and historical significance, increasingly struggle to support the demands of today's data-driven organizations. In conclusion, the migration from legacy databases to hybrid cloud environments represents a pivotal step in the modernization journey of contemporary enterprises. By adopting this framework, organizations can ensure that their data architectures evolve in alignment with emerging technologies, business strategies, and regulatory landscapes. This study ultimately reinforces that hybrid cloud adoption when guided by a clear, structured framework— enables organizations to optimize performance, enhance scalability, reduce costs, and drive innovation, while safeguarding the integrity and continuity of essential legacy systems.

REFERENCES

1. *J. Shahithya (2023), "Cloud Database: Empowering Scalable and Flexible Data Management",Quing: International Journal of Innovative Research in Science and Engineering", ISSNno:2583-3871, Vol.2, No.1, Pages.1-23. https: //doi.Org/10.54368/qijirse.2.1.0007*
2. *Satish S R V Karuturi (2023), "Database Security Issues and Challenges in Cloud Computing", International Journal on Recent and Innovation Trends in Computing and Communication,ISSNno:2321-8169,Vol.11(11),Pages.937-943.DOI:10.17762/ijritcc.v11i11.10396*
3. *Norah Farooqi (2022), "A Systematic Literature Review on Security Challenges In A Hybrid Cloud Database", International Journal of Engineering & Technology, ISSNno:2227-524X,Vol.11(1),Pages.10-13. DOI: 10.14419/ijet. v11i1.31911*
4. *Zayaraz G. (2021), "A Robust Lightweight Data Security Model for Cloud Data Access and Storage," International Journal*

of Information Technology and Web Engineering (IJITWE), ISSNno:1554-1053,Vol.16(3),Pages.39-53.

5. *Song Wang (2020), "Teaching Exploration of Case-Based Data Modeling Optimization for Database System", Open Journal of Social Sciences, ISSNno: 2327-5960, Vol.8,No.3,Pages.514-521*
6. *S. Silas Sargunam (2016), "Cloud Computing-System Implementation for Business Applications", Circuits and Systems,ISSNno:2153-1293,Vol.7,No.6, Pages.891-896.*
7. *Kashish Ara Shakil (2015), "Cloud Database Management System Architecture", UACEE International Journal of Computer Science and its Applications,ISSNno:2250-3765,Vol.3,Issue.1,*
8. *Horacio Leone (2015), "Migration of Legacy Systems to Cloud Computing", Electronic Journal of SADIO,ISSNno:1514-6774,Vol.14.*
9. *E.E. Hassanein (2018), "A proposed hybrid model for adopting cloud computing in e-government", Future Computing and Informatics Journal, ISSNno:2314-7296, Vol.3, Issue.2, Pages.286-295. https://doi.org/10.1016/j. fcij. 2018.09.001*
10. *Nova Ahmed (2013), "Efficient And Reliable Hybrid Cloud Architecture For Big Database", International Journal on Cloud Computing: Services and Architecture (IJCCSA), ISSNno:2231-5853, Vol.3, No.6, DOI: 10. 51 21 /ij cc sa.20 13.3602*