TOWARDS BLOCKCHAIN-BASED SECURE STORAGE AND TRUSTED DATA SHARING SCHEME FOR IOT ENVIRONMENT

[1]***Manikeshwari,*** *Master of Computer Application BKIT-Bhalki*
[2]***Prof . Yogesh V.Gundge,*** *Master of Computer Application BKIT-Bhalki*

Abstract - Data is and will continue to be a vital component of every contemporary application that we envision. Looking forward, the potential of machine learning and artificial intelligence will further increase the quantities. Data sharing presents a number of issues, which may be generally classified as follows: data format and meaning; legal requirements; privacy; data security; and worries about unintended repercussions of data sharing. It is not a simple topic to address since it involves not only technological issues but also social, economical, ethical, and regulatory concerns.

This necessitates the development of sharing frameworks that solve technological obstacles, include regulatory frameworks, and anticipate and address concerns about the fairness and justice of results in order to preserve consumer and community confidence. This study presents a paradigm for data sharing that includes several ecosystems, with blockchain technology serving as the system's backbone. Because blockchain addresses the fundamental challenges of trust, data correctness, and dependability, it goes on to give a revolutionary solution for data sharing. In today's world, data processing, distribution, and storage all take place mostly in the cloud. The present IoT cloud-centric architecture has led to the quick creation of IoT applications, however it has also into a plethora of separate data silos, which prevents it1s full potential. IoT applications of comprehensive data-driven analytics. This study examines demonstrate a distributed access control and data management IoT design based on blockchain. We move on from the present trust model, which gives a third party access to our data, instead of centralized trusted authority, give users ownership of data. We have adapted our design for IoT data streams and allows for safe data sharing. We make access reliable and secure. control management with an auditable blockchain technology from the storage layer's distributed access control layer. We make it easier to store time-series IoT data at the network's edge. through a managed locality-aware decentralized storage system through the use of blockchain technology

***Key Words*:** Blockchain, IOT, Storage

INTRODUCTION

These words Data-intensive industries include the medical/healthcare, banking, and IoT sectors where a significant amount of data is generated, transmitted, stored, and retrieved on a daily basis [6].

During the previous decade, data was gathered, extracted, converted, and fed into Datawarehouse (DWH) from a variety of source systems. Data reconciliation between the source system and DWH is then performed.

The data would be different and not the same if it were shared with multiple parties, which is a problem once it is created and when it needs to be shared via a network or the internet. This occurs because data synchronization frequently takes place towards the end of the day and is not instantaneous. The process of reconciliation costs money. Additionally, there is always a chance that the data will be altered, and double spending on financial transactions is always a worry. For current applications, traditional data exchange techniques are typically expensive in terms of security, energy use, and processing overhead. These days, the majority of apps prefer the cloud because of the convenience of high availability and cost savings. However, there are certain restrictions when it comes to addressing security and privacy issues in a setting where cloud computing is becoming more prevalent. [6]

Furthermore, a lot of cutting-edge frameworks are very centralized, making them less than ideal for sharing data in modern applications due to issues with scalability, security, the lack of a consensus mechanism, single points of failure, and user privacy and consent. Because of this, current applications require distributed security and privacy protection, consensus-based data sharing, and tamper-proof, time stamp-based data storage. Following the literature review, we have highlighted the work on the data sharing framework that has been done in several fields.

SYSTEM ANALYSIS:

Existing System:

Shunrong Jiang [3] shows the security issues when deploying NDN to VANETs for media distribution in V-NDN and suggests suitable solutions (ESAC). To begin with, researchers develop a proxy re-encryption technique that provides identity management, revocation, and updating even in the absence of a reliable source. Pseudonyms and an identifier-based signature are used by researchers to address the issue of anonymous authentication and validity checking. Researchers offer a strategy that uses a hashed certificate as an incentive to ensure NDN's utility in VANETs. The security study's findings indicate that ESAC can deliver the required level of security for use in V-NDN. The results of the simulations further show that the suggested secure technique has no effect on the network's effectiveness.

Proposed System

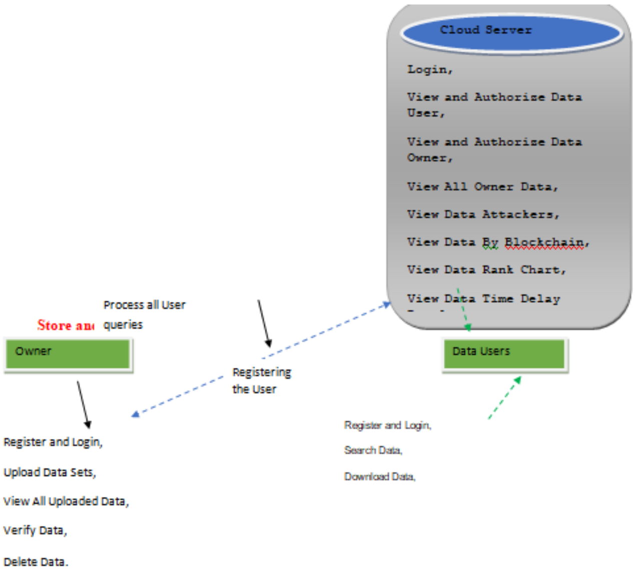
We provide a block chain-based system for data exchange. Issuer and verifier are only two of the stakeholders involved. These are the users who would contribute, modify, or retrieve this data from the system. They might be either people or organizations. The user intends to upload the most recent documents or artifacts to a system built on a blockchain. Depending on the use case, multiple roles would exist in the system. Let's assume that for the purpose of data exchange in a VISA application for a certain nation, the country's embassy office would play one function, the visa applicant another, and so on, depending on the usecase. The data format follows next, where we advise using structured data that can be utilized with any relational database.

The program could be interportable. The program, which is based on roles that may be assigned to users, will handle all access rights granted in the system.

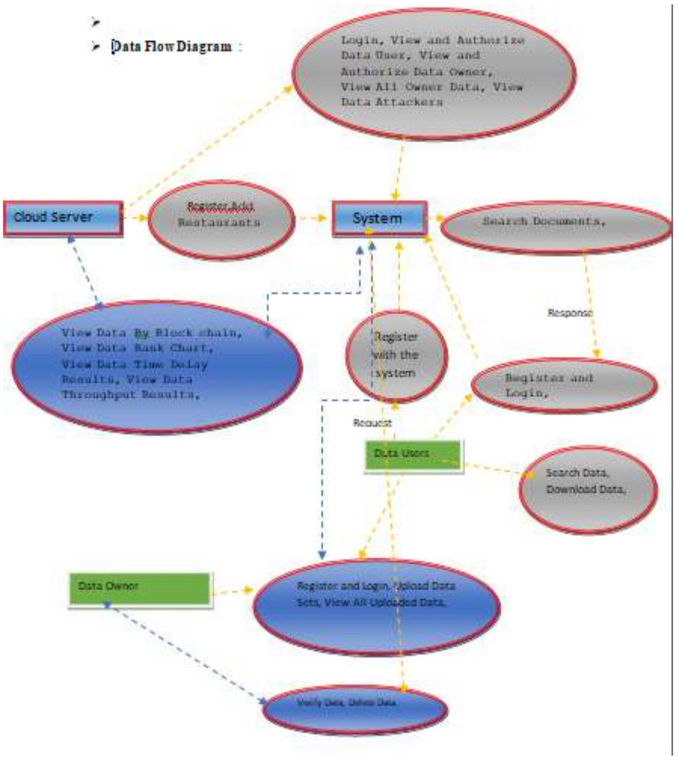
The management of the CI (Confidentiality and Integrity) component of security is where blockchain is most useful. Redundancy may be employed for availability at the application architectural level; it is not covered in this work.

The framework's implementation and metrics analysis from a further optimization and scalability perspective are the next phases.

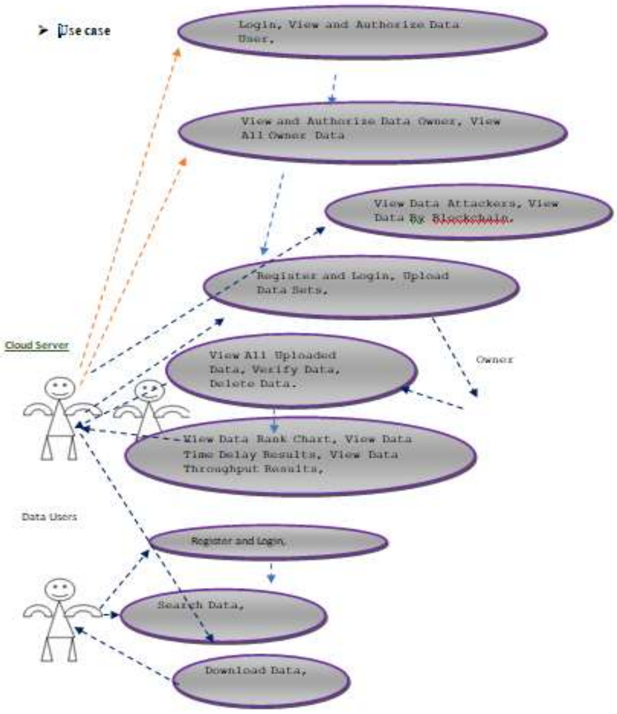
ARCHITECTURE



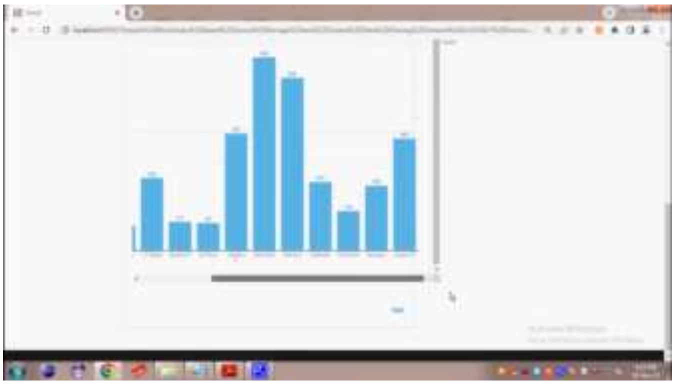
- Data Flow Diagram :

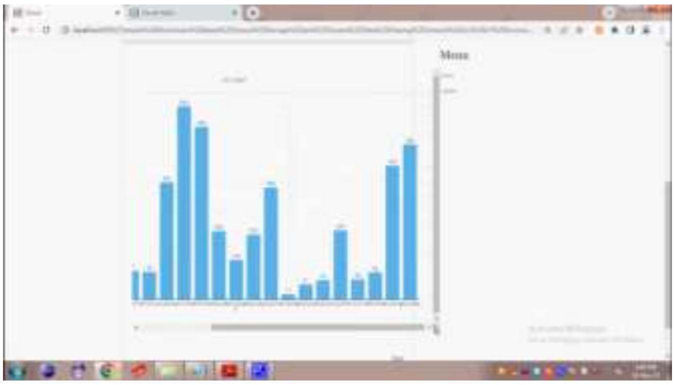

Login, View and Authorize Data User, View and Authorize Data Owner, View All Owner Data, View Data Attackers
Cloud Server
Register Add Restaurants
System
Search Documents,
View Data By Block chain, View Data Rank Chart, View Data Time Delay Results, View Data Throughput Results,
Register with the system
Response
Register and Login,
Request
Data Users
Search Data, Download Data,
Data Owner
Register and Login, Upload Data Sets, View All Uploaded Data,
Verify Data, Delete Data

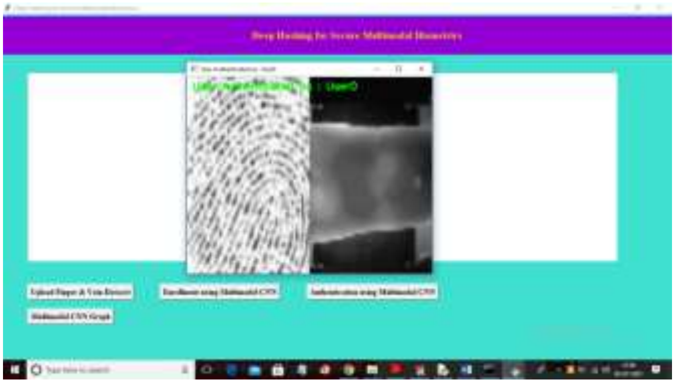
- Use case


Login, View and Authorize Data User,
View and Authorize Data Owner, View All Owner Data
View Data Attackers, View Data By Blockchain,
Register and Login, Upload Data Sets,
Cloud Server
View All Uploaded Data, Verify Data, Delete Data.
Owner
View Data Rank Chart, View Data Time Delay Results, View Data Throughput Results,
Data Users
Register and Login,
Search Data,
Download Data,

Results and Analysis:






Deep Hashing for Secure Multimodal Biometrics
User0
Upload Finger & Vein Dataset
Enrollment using Multimodal CNN
Authentication using Multimodal CNN
Multimodal CNN Graph

Conclusion:

In this research, we suggested a block chain-based data sharing architecture that is highly general and may be used in any field where it is difficult to share sensitive data among several parties. With the help of this framework, data is transferred securely, and data privacy is maintained. The methods for communication and authentication should be further explored, and this research effort should be expanded. As we go forward, we'll keep implementing the system based on this framework and conduct research to improve optimization and gather empirical data for more investigation and research.

Bibliographic Citation

[1] Ajay Kumar Shrestha(&) and Julita Vassileva, "Blockchain-Based Research Data Sharing Framework for Incentivizing the Data Owners" Springer Nature 2018, a division of Springer International Publishing AG ICBC 2018, S. Chen et al. (Eds.), LNCS 10974, 259–266.

[2] Venkatraman Ramakrishna, Ernie GS Teo, Chun Hui Suen, Peter Ilfrich, Dain Liffman, Christian Vecchiola, Praveen Jayachandran, Apurva Kumar, Fabian Lim, Karthik Nandakumar, Zhengquan Qin, and Kumar Bhaskaran 2018 IEEE International Conference on Cloud Engineering, "Double-Blind Consent-Driven Data Sharing on Blockchain"

[3] "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," by Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang. IEEE's Sixth International Congress on Big Data in 2017

[4] "Blockchains and Smart Contracts for the Internet of Things," by KONSTANTINOS CHRISTIDIS (Graduate Student Member, IEEE) AND MICHAEL DEVETSIKIOTIS (Fellow, IEEE). Digital Object Identifier 0.1109/ACCESS.2016.2566339 for IEEE Access

[5] "Blockchain Standards for Compliance and Trust," by Ashiq Anjum, Manu Sporny, and Alan Sill. Published by the IEEE Computer Society, IEEE CLOUD COMPUTING [6] Esposito, Christian Esposito, Christian College of Salerno Salerno's Alfredo De Santis University Genny Tortora Salerno University Hong Kong's Henry Chang University Kim-

Kwang "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" by Raymond Choo, University of Texas at San Antonio.
cloud computing IEEE IEEE CS and IEEE ComSoc jointly published in January/February 2018

[7] Bin Yu CSIRO Data61, Monash University Liming Zhu, Jarod Wright, and Surya Nepal CSIRO Data61 Joseph Liu University of Monash Ranjan Rajiv "TrustChain: Establishing Trust in the IoT-based Applications Ecosystem Using Blockchain," Newcastle University. Cloud computing with IEEE Copublished in July/August 2018 by the IEEE CS and IEEE ComSoc

[8] The authors of "KYC Optimization Using Distributed Ledger Technology" are Jose' Parra Moyano and Omri Ross. Bus Inf Syst Eng 59(6):411-423 (Springer, 2017).

[9] "Towards decentralized data storage in general cloud platform for meta-products," Ajay Kumar Shrestha (&) and Julita Vassileva. November 10–11, 2016, Blagoevgrad, Bulgaria, BDAW'16 2016 ACM. 16/11. ISBN 978-1-4503-4779-2