IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Adoption of Blockchain in Cyber Security

Farhana A. J[1], Nisha A[2], Harikrishnan S R[3]
Student, MCA, CHMM College for Advanced Studies, Trivandrum, India [1]
Assistant Professor, MCA, CHMM College for Advanced Studies, Trivandrum, India [2]
Associate Professor, MCA, CHMM College for Advanced Studies, Trivandrum, India [3]

Abstract: *In recent decades, blockchain has (slowly) become one of the most frequently discussed methods for securing data storage and transfer through decentralized, trustless, peer-topeer systems. We present a comprehensive method of how blockchain technology is applied to provide security over the network and to counter ongoing threats as well as increasing cybercrimes and cyber-attacks. We focused on blockchain technology for cyber defence. With digital innovation on military and social infrastructure, cyber threats are not avoidable. Blockchain technology is one of the emerging technologies for security in defence. It has a decentralized nature, so a blockchain ensures data processing integrity. It significantly helps secure system reliability against cyber threats. We provided a scope of cyber defence and reviewed blockchain research and development trends under the defined cyber defence. And then, we explored the potential concerns in the use of blockchain based on recent research and blockchain methodologies. The blockchain-based decentralized storage system splits users' files into varied tiny chunks of information, mentioned as "blocks". It then encrypts every block with a unique hash or with public-private keys and distributes the blocks across multiple computers or "nodes". This method of distributing information across the network of node is called sharding. Similarly, all information is distributed and stored across decentralized locations. If hackers attempt to breach these locations, they encounter encrypted blocks of data. Furthermore, they can only access a fragment of the information, not the complete file. This is how blockchain-based decentralized storage systems ensure data security.*

Keywords: Blockchain Technology, Data Security, Decentralized Storage, Cyber Defense, Encryption

I. INTRODUCTION

In recent decades, blockchain has increasingly emerged as a prominent method for securing data storage and transfer through decentralized, trustless peer-to-peer systems. Our study provides a thorough examination of how blockchain technology enhances network security and addresses the growing threats of cybercrimes and attacks. We specifically focus on blockchain for cyber defense, recognizing that with advancements in military and social infrastructure, cyber threats are unavoidable. Blockchain, with its decentralized architecture, ensures data processing integrity and significantly strengthens system reliability against cyber threats. We reviewed the scope of cyber defense, analyzed trends in blockchain research and development, and investigated potential concerns associated with blockchain usage based on recent findings and methodologies. Blockchain-based decentralized storage systems operate by splitting users' files into small segments called "blocks," each of which is encrypted with a unique hash or public-private keys. These encrypted blocks are then distributed across various computers or "nodes." This method, known as sharding, ensures that data is spread across multiple decentralized locations. Consequently, if hackers try to access these locations, they encounter only encrypted blocks and can retrieve only partial information, not the complete file. This method effectively preserves data security through blockchain-based decentralized storage.

II. LITERATURE SURVEY

The literature on blockchain technology emphasizes its transformative impact on data security and cyber defense. Initially introduced by Nakamoto for cryptocurrencies, blockchain has evolved to address broader security needs by leveraging decentralized, tamper-proof ledgers. Research highlights its effectiveness in decentralized storage systems, where data is split into encrypted blocks and distributed across a network, significantly reducing the risk of breaches. Studies also showcase blockchain's potential to enhance system reliability and defend against various cyber threats

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

through decentralized consensus and smart contracts. However, challenges such as scalability and implementation vulnerabilities remain. Ongoing research is focused on optimizing blockchain's performance and integrating it with emerging technologies to further bolster cyber defense capabilities

III. WORKING OF PROPOSED SYSTEM

In the proposed approach, users begin by logging into the system and selecting a server plan. They then submit a request to the Cloud Service Provider (CSP) for access to the desired cloud services. Upon approval of the request by the CSP, users can engage in various activities on the cloud, such as uploading, deleting, sharing, or updating files. The system meticulously generates and encrypts log entries, capturing details such as the user's email, MAC address, IP address, and activity logs. These logs are reviewed by both the CSP and investigators to pinpoint the attacker's IP address. To address insider threats, the system is designed with threshold-based detection mechanisms for DDoS attacks. If an insider surpasses these predefined thresholds, the system will display relevant user information, thus facilitating effective monitoring and response. The security framework of the system relies on a password-based AES encryption algorithm with a 256-bit key. This algorithm incorporates salt and two iterations to bolster security, making it more challenging for attackers to compromise the system. Overall, the system provides a high level of security, transparency, and operational efficiency. It features low computational complexity while offering robust protection against various forms of cyberattacks, including brute-force, eavesdropping, man-in-the-middle, offline dictionary, and collusion attacks. Additionally, the system boasts several notable advantages. It employs a dedicated Cloud server that becomes operational only after a client registers, ensuring that resources are allocated effectively and securely. This server performs unidirectional encryption and decryption, which significantly enhances the security of data both during transmission and while stored. As a result, the system guarantees comprehensive end-to-end user privacy and maintains strong privacy protections at the Cloud server level.

IV. TECHNOLOGY USED

Visual studio 2019

Visual Studio 2019 is a powerful integrated development environment (IDE) developed by Microsoft, designed to streamline the software development process. It provides a comprehensive suite of tools and features to support a wide range of programming languages and development tasks, making it a popular choice among developers. One of the key features of Visual Studio 2019 is its enhanced IntelliSense, which offers smarter code completion, parameter info, quick info, and member lists. The IDE also includes a robust debugging environment that allows for easy identification and resolution of code issues. It supports a variety of debugging techniques, including live debugging, snapshot debugging, and the ability to set breakpoints and inspect variables. Visual Studio 2019 introduces improved performance and a more streamlined user interface compared to its predecessors. The IDE includes a customizable start window, which provides quick access to recent projects and various development tools. Additionally, the new version supports advanced code navigation features, such as code maps and enhanced search functionalities, which make it easier to manage and understand complex codebases.Another significant enhancement in Visual Studio 2019 is its support for modern development practices, including integration with Azure DevOps and GitHub for version control and continuous integration/continuous deployment (CI/CD) pipelines. Overall, Visual Studio 2019 is a versatile and feature-rich IDE that caters to both individual developers and large teams. Its advanced features, improved performance, and support for modern development workflows make it an essential tool for effective and efficient software development.

C#.net

C# (C-Sharp) is a modern, object-oriented programming language developed by Microsoft as part of its .NET framework. Designed for building a wide range of applications, C# combines the power of C++ with the simplicity of Visual Basic, providing a versatile tool for developers. It is widely used for developing Windows applications, web services, and enterprise software.C# features strong type checking, garbage collection, and support for component-oriented programming, which enhances code reliability and reduces common programming errors. Its syntax is clean and expressive, making it accessible for both novice and experienced developers. The language supports object-oriented principles such as encapsulation, inheritance, and polymorphism, enabling the creation of reusable and modular

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

code.One of C#'s key strengths is its integration with the .NET framework, which provides a vast library of pre-built components and a common language runtime (CLR) that handles program execution. C# also supports asynchronous programming through async/await keywords, simplifying the development of responsive and scalable applications. With tools like Visual Studio, C# developers benefit from an advanced IDE that offers features like code completion, debugging, and performance profiling, streamlining the development process and improving productivity.

Microsoft sql server 2008

Microsoft SQL Server 2008 is a robust relational database management system (RDBMS) developed by Microsoft, launched in August 2008. A standout feature of SQL Server 2008 is the SQL Server Management Studio (SSMS), which provides an integrated environment for database administration, query execution, and performance tuning. The system also includes SQL Server Integration Services (SSIS), which facilitates the extraction, transformation, and loading (ETL) of data, streamlining data integration and migration processes.Security is a major focus in SQL Server 2008.The system also supports detailed auditing, allowing organizations to track and review database activities for compliance and security purposes.SQL Server 2008 enhances reporting capabilities through SQL Server Reporting Services (SSRS), which offer powerful tools for creating interactive reports and dashboards, aiding in data-driven decision-making. Additionally, Data Compression features help optimize storage efficiency and performance by reducing the size of database objects.To ensure high availability and disaster recovery, SQL Server 2008 includes Database Mirroring and Backup Compression, which protect data integrity and availability in case of system failures.In summary, Microsoft SQL Server 2008 provides a comprehensive set of tools and features that support effective data management, robust security, and advanced reporting, making it a valuable resource for a wide range of data-driven applications.Overall, Microsoft SQL Server 2008 offers a comprehensive suite of tools and features that address a wide range of data management needs, combining robust performance, enhanced security, and sophisticated reporting functionalities.

Open cv

OpenCV (Open Source Computer Vision Library) is a widely used open-source library designed for real-time computer vision and image processing. Developed initially by Intel and now maintained by the OpenCV community, it provides a comprehensive set of tools and algorithms to handle a variety of visual data tasks.OpenCV supports numerous programming languages, including C++, Python, and Java, making it versatile and accessible for different development environments. The library includes functionality for image and video analysis, object detection, feature extraction, machine learning, and more. It facilitates tasks such as facial recognition, motion tracking, and image enhancement, and it integrates well with other machine learning frameworks and deep learning libraries like TensorFlow and PyTorch.The library is widely adopted in academic research, industry applications, and hobbyist projects due to its extensive capabilities and active community support. It offers a robust set of functions for image manipulation, geometric transformations, and data visualization, providing developers with the tools needed to create sophisticated computer vision applications. OpenCV's efficiency and flexibility make it a valuable resource for anyone working in the field of computer vision and image processing.

Blockchain technology

Blockchain technology is a decentralized digital ledger system that securely records and manages transactions across a network of computers. Its primary innovation lies in removing the necessity for a central authority to oversee and verify records. Initially created for cryptocurrencies such as Bitcoin, blockchain has since gained recognition for its potential applications in a wide range of industries. A blockchain consists of a series of blocks, each containing a list of transactions. Blocks are linked to one another using cryptographic hashes, forming a continuous chain. This chaining process ensures that once data is recorded, it cannot be altered without modifying all subsequent blocks, which requires consensus from the majority of network participants. This immutability is crucial for the technology's security. The decentralized nature of blockchain is achieved by a network of nodes, where each node holds a complete copy of the entire blockchain. This setup provides transparency and redundancy. When a new transaction occurs, it is broadcast to all nodes, which use consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), or Byzantine Fault

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Tolerance (BFT) to validate and record the transaction. These mechanisms help ensure the network agrees on the transaction's validity and maintains ledger integrity. Blockchain offers significant benefits, including enhanced security through its cryptographic and decentralized nature, which mitigates risks of tampering and fraud. It also promotes transparency and traceability, as all transactions are recorded and accessible for auditing. This is particularly valuable in sectors like supply chain management, where tracking the movement of goods is essential. Additionally, blockchain supports smart contracts—self-executing agreements with terms written into code that automatically enforce and execute when conditions are met. This feature reduces the need for intermediaries and minimizes potential disputes, with applications in finance, real estate, and legal agreements. Despite its advantages, blockchain faces challenges such as scalability, where the growing size of the blockchain can impact performance and storage. Energy consumption associated with certain consensus mechanisms, particularly Proof of Work, raises environmental concerns. Privacy is another issue, as the transparency of public blockchains can expose sensitive information. Nevertheless, blockchain technology continues to evolve and expand beyond cryptocurrencies. It is being explored for use in healthcare to securely manage patient records, in finance to enhance payment systems and reduce fraud, and in government to improve transparency and combat corruption. As advancements continue, blockchain has the potential to transform various industries by providing a secure, transparent, and decentralized approach to managing and recording transactions.

Advanced Encryption Standard (AES) algorithm

The Advanced Encryption Standard (AES) algorithm is widely used in blockchain technology to enhance data security and privacy. AES is a symmetric key encryption algorithm that employs a single key for both encryption and decryption, making it a fast and efficient method for protecting sensitive information. In the context of blockchain, AES is utilized to ensure that data stored on the blockchain remains confidential and secure from unauthorized access. When data is written to the blockchain, it is often encrypted using AES before being recorded. This process involves converting the plaintext data into ciphertext using a secret key. Only users with the appropriate decryption key can revert the ciphertext back to its original plaintext form. This encryption process ensures that even if a blockchain node is compromised, the data remains protected as long as the encryption key is secure.AES's role in blockchain extends to securing transaction data, smart contracts, and other critical information. By integrating AES encryption, blockchain networks can maintain data integrity while safeguarding sensitive information from potential breaches. This encryption approach complements blockchain's inherent security features, such as its decentralized structure and consensus mechanisms, by adding an additional layer of data protection.

V. DATABASE DESIGN

Database design is a fundamental aspect of software system development. At the top of the hierarchy, the database functions as a collection of interrelated files designed for real-time processing. It holds essential data for solving problems and supports concurrent access by multiple users. The primary aim of database design is to ensure that data access is efficient, cost-effective, and flexible for users.The process of database design involves defining and specifying the structure of data within a client/server system. A Database Management System (DBMS) is instrumental in organizing and protecting data, keeping it separate from hardware, software, and other programs. The DBMS distinguishes between logical data (as perceived by applications) and physical data (stored on direct access storage devices), emphasizing the importance of this separation.In my project, Microsoft SQL Server 2005 was used to implement the data storage component. A critical aspect of the database design was determining the appropriate tables to use.

Login

Field Name	Data Type	size	Constraint	Description
Username	Varchar	12	Primary key	Username
Password	Varchar	12	Not null	Password of user
Status	int	2	Not Null	Status of login

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

Datadb

Field Name	Data Type	size	Constraint	Description
fileid	int	4	Primary key	File Identification
username	Varchar	30	Foreign key	Username
Filename	varchar	30	Not Null	File Name
Tbdate	varchar	30	Not Null	File Updated date
Code	varchar	30	Not Null	File encrypted
Priority	varchar	30	Not Null	Priority of file
Filepassword	varchar	30	Not Null	Password of file
Block1	varchar	30	Not Null	Block details
Block2	varchar	30	Not Null	Block details
status	int	4	Not Null	Status of file

Emptb

Field Name	Data Type	size	Constraint	Description
empid	int	4	Primary key	Employee Identification
empusername	varchar	30	Foreign key	Employee username
pwd	varchar	30	Not Null	Password
name	varchar	30	Not Null	Name
gender	varchar	30	Not Null	Gender
phone	varchar	30	Not Null	Phone number
email	varchar	30	Not Null	Email ID
dob	varchar	30	Not Null	Date of birth
Address	varchar	30	Not Null	Address
Designation	varchar	30	Not Null	Designation of employee
status	int	4	Not Null	Status of file

Sharetb

Field Name	Data Type	size	Constraint	Description
shareid	int	4	Primary key	Share id
fileid	int	4	Foreign key	File ID
shareduser	Varchar	30	Foreign key	Shared username
username	Varchar	30	Foreign key	Sender username

VI. FUTURE WORK

Existing systems have often provided limited protection for user-sensitive information. Our system, however, significantly enhances security through advanced encryption and hashing techniques specifically designed to safeguard sensitive data. In addition to these measures, it features mechanisms for detecting insider DDoS attacks, further strengthening its security capabilities. All logs within our system are fully encrypted, ensuring that they cannot be altered by unauthorized parties, thus preserving the integrity of the log data.This robust security framework not only secures data but also offers a foundation for addressing a broader spectrum of cloud-based threats. For example, the system can be extended to detect complex attacks such as man-in-the-cloud or insider threats. Furthermore, integrating

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

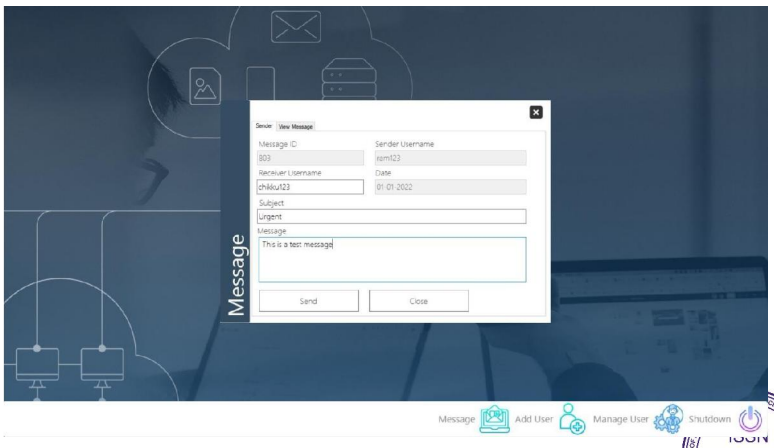
additional log analysis tools could improve the system's ability to identify various cloud attacks, enhancing its effectiveness in cloud forensics. Such expansions would provide a more comprehensive approach to securing cloud environments and tackling emerging security challenges.

VII. RESULT

Admin Page

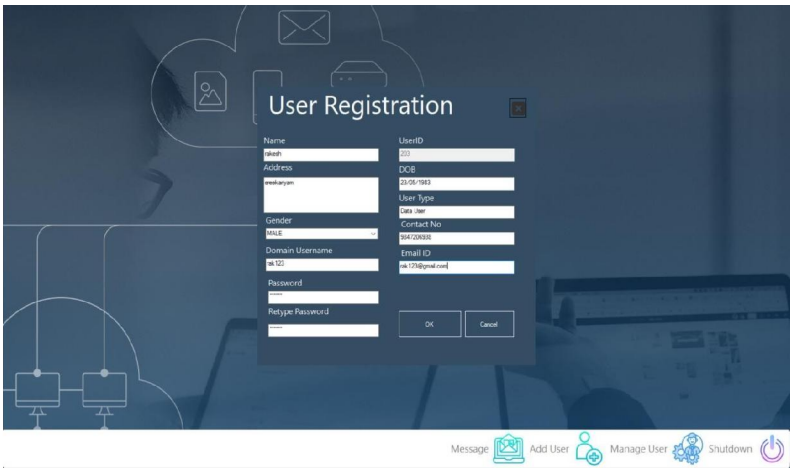
Domain registration

Communication

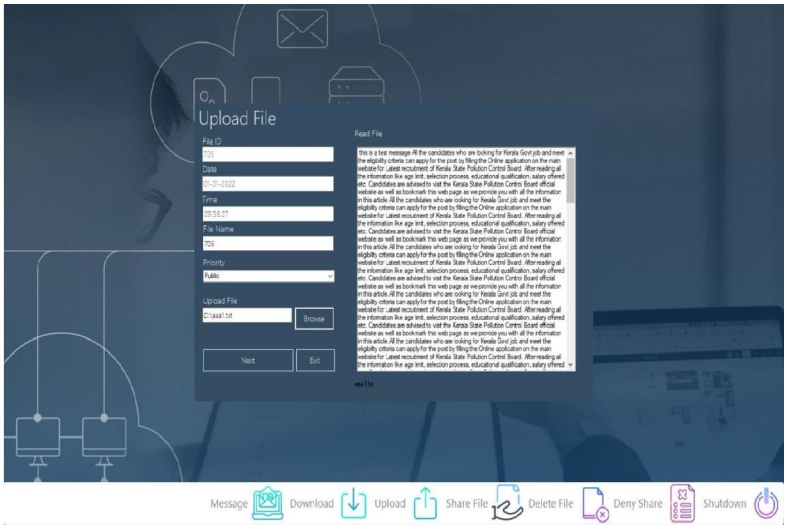


IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

User registration



Upload file to cloud



VIII. SUMMARY

In the proposed work, a secure log system is designed which will provide secure and reliable logs to investigators for cloud forensics. The Secretness and Privacy of cloud users will be preserved by using a searchable encryption technique. The encryption purpose system uses a password-based AES algorithm which contains iteration, salt & provides MD5 hashing on encrypted IP address. This proposed a system that is capable of capturing large amounts of DDos traffic and store the logs they produce on a Distributed File System. Then the system can crossreference those logs with a dataset to establish a ground truth and generate a Model that is capable of predicting attacks in a distributed manner. As such, we believe this system should increase security standards and provide flexibility and scalabitility when integrated into a network attack prediction or prevention environment

REFERENCES

[1]. B. P. Laxmi and A. Chilambuchelvan, ‘‘GSR: Geographic secured routing using SHA-3 algorithm for node and message authentication in wireless sensor networks,’’ Future Gener. Comput. Syst., vol. 76, pp. 98–105, Nov. 2017.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, August 2024

[2]. A Alromih, M. Al-Rodhaan, and Y. Tian, ''A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for Internet of Things applications,'' Sensors, vol. 18, no. 12, p. 4346, Dec. 2018.

[3]. H. K. D. Sarma, A. Kar, and R. Mall, ''A hierarchical and role based secure routing protocol for mobile wireless sensor networks,'' Wireless Pers. Commun., vol. 90, no. 3, pp. 1067–1103, Jun. 2016.

[4]. A Rachedi and A. Hasnaoui, ''Advanced quality of services with security integration in wireless sensor networks,'' Wireless Commun. Mobile Comput., vol. 15, no. 6, pp. 1106–1116, Apr. 2015.

[5]. G. D. Devanagavi, N. Nalini, and R. C. Biradar, ''Secured routing in wireless sensor networks using fault-free and trusted nodes,'' Int. J. Commun. Syst., vol. 29, no. 1, pp. 170– 193, Jan. 2016.