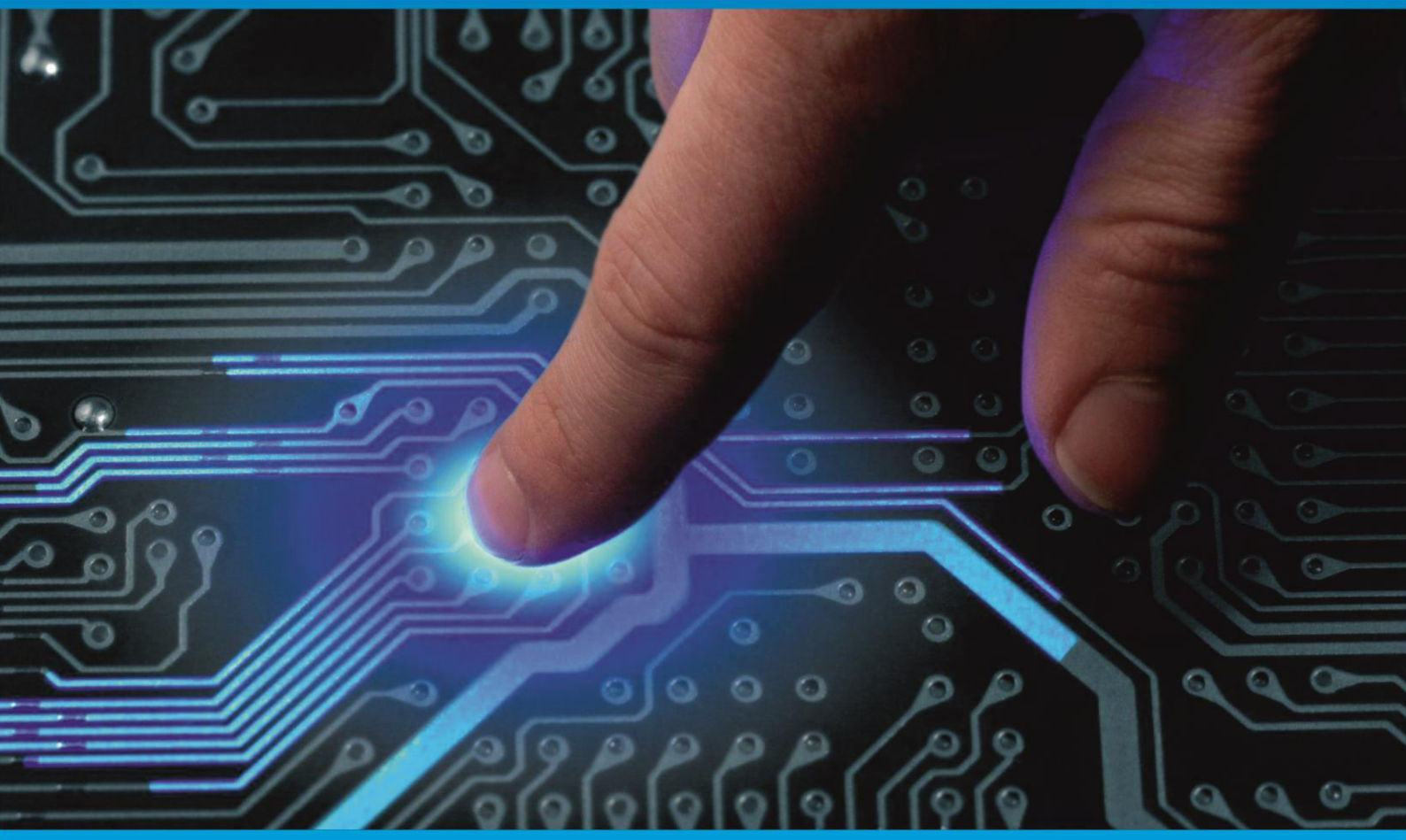
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

Student Forum Using Ethereum Blockchain

Paramjeet Singh Kathuria[1], Kaushal Chaudhari[2], Saurabh Pardeshi[3], Koushik Debnath[4], Prof. Madhuri Yadav[5]

Department of Computer Engineering, Sinhgad College of Engineering (Vadgaon,Bk), Savitribai Phule Pune University, Pune, Maharashtra, India[1,2,3,4]

Department of Computer Engineering, Sinhgad College of Engineering (Vadgaon,Bk), Savitribai Phule Pune University, Pune, Maharashtra, India[5]

ABSTRACT: Block-chain is an emerging technology for distributed and data sharing across a large network of un-trusted participants. In today's day in data storage system is growing fast also as well as the data need to store securely [5]. It allows new forms of distributed software architectures. Although the technology was mainly accepted in digital currency in initial days, but it is a promising technology for other areas too. This work is designed using block chain concept and key-based cryptographic technique. Block chain technology has emerged as one of the major trends in the field of security and message transfer. This technology is also the foundation of many other popular technologies like crypto currency. Hashing techniques used (like SHA-1,SHA-256) gives it an unparalleled security advantage. Main aim of our project is to demonstrate the potential of block chain technology in secure transfer of messages (both multimedia and text) and create a platform(web based application)for students and faculty community to exchange information about the current happenings at both college and university level.

KEYWORDS : Block chain, Data Security, Encryption, Smart Contract, Cloud Storage.

I. INTRODUCTION

Block-chain is an emerging technology for distributed and data sharing across a large network of un-trusted participants. In today's day in data storage system is growing fast also as well as the data need to store securely [5]. It allows new forms of distributed software architectures. Although the technology was mainly accepted in digital currency in initial days, but it is a promising technology for other areas too. This work is designed using block chain concept and key-based cryptographic technique.

Blockchain technology has emerged as one of the major trends in the field of security and message transfer. This technology is also the foundation of many other popular technologies like cryptocurrency. Hashing techniques used (like SHA-1,SHA-256) gives it an unparalleled security advantage.

1.1. Problem Statement/Objective

To build and implement student forum using ethereum block chain.

1.2. Aim

Main aim of our project is to demonstrate the potential of blockchain technology in secure transfer of messages (both multimedia and text) and create a platform(web based application)for students and faculty community to exchange information about the current happenings at both college and university level.

II. RELATED WORK

Privacy-preserving Search over Encrypted Personal Health Record in Multi-Source [1], In this paper- 1.Multi-source CB-PHR system in which multiple data providers such as hospitals and physicians are authorized by individual data owners to upload their personal health data to an untrusted public cloud 2. Multi-Source Order-Preserving Symmetric Encryption (MOPSE) scheme whereby the cloud can merge the encrypted data indexes from multiple data providers without knowing the index content

Efficient Searchable Symmetric Encryption for Storing Multiple Source Dynamic Social Data on Cloud [2] In this paper- 1. Dynamic Searchable Symmetric Encryption (DSSE) is an advanced cryptographic primitive addressing the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

above issue, which maintains efficient keyword search over dynamic encrypted data without disclosing much information to the storage provider.

A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data [3], In this paper- This paper propose a "Greedy Depth-first Search" algorithm to provide efficient multi-keyword ranked search.

CrowdBC: A Blockchain-based Decentralized Framework for Crowdsourcing [4], In this paper- Use decentralized framework for crowdsourcing systems.

III. PROPOSED SYSTEM

In proposed system, to store all student information, notes, previous implemented project data with synopsis in the system. The student registers details first. The details are name, email, password, roll no, branch and year. This saves time in the long term because there is no need to re-organize, re-format, or try to remember details about notes and projects. It also increases research efficiency since both the data collector and other researchers will be able to understand and use well-annotated data in the future.

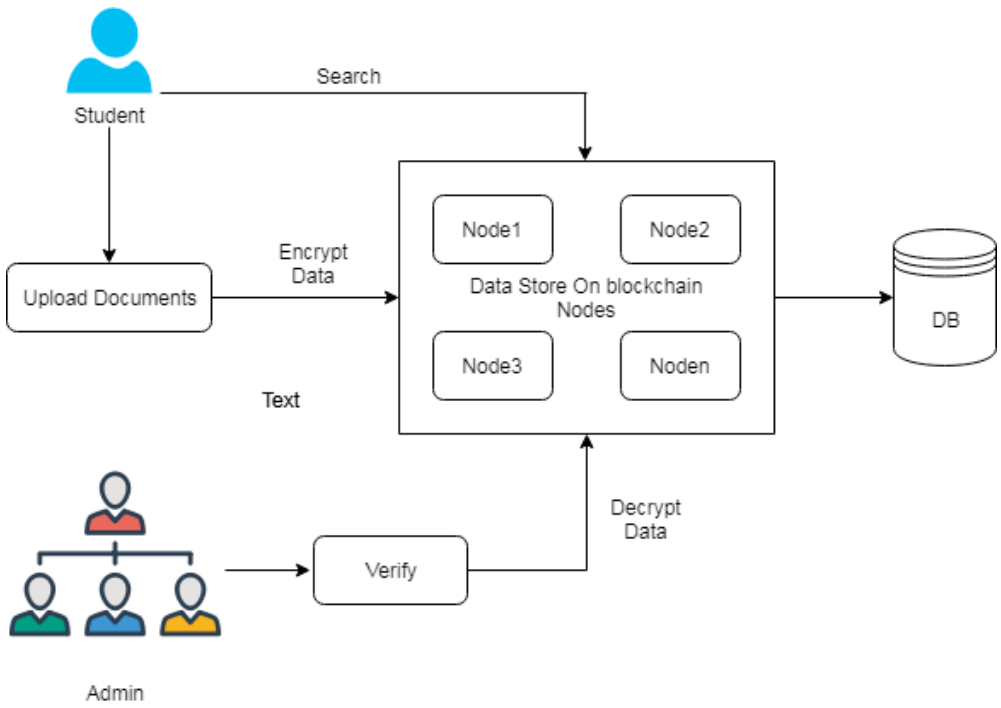


Fig 1: System Architecture

IV. MATHEMATICAL MODEL

Let us consider S as a system for Data storage management.
S=
INPUT:
Identify the inputs
F= f1, f2, f3 ....., FN— F as set of functions to execute commands.
I= i1, i2, i3—I sets of inputs to the function set
O= o1, o2, o3.—O Set of outputs from the function sets,
S= I, F, O
I = file uploaded by the user
O = Output i.e. store data
F = Functions implemented to get the output

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

Space Complexity:
The space complexity depends on Presentation and visualization of discovered patterns.
More the storage of data more is the space complexity.
Time Complexity:
Check No. of patterns available in the datasets= n
If (n(1)) then retrieving of information can be time consuming. So the time complexity of this algorithm is O (nˆn).
= Failures and Success conditions.
Failures:
1. Huge database can lead to more time consumption to get the information.
2. Hardware failure.
3. Software failure.
Success:
1. Search the required information from available in Datasets.
2. User gets result very fast according to their needs.

V.ALGORITHAMS

1. AES Algorithm for Encryption.
AES (advanced encryption standard).It is symmetric algorithm. It used to convert plain text into cipher text .The need for coming with this algo is weakness in DES. The 56 bit key of des is no longer safe against attacks based on exhaustive key searches and 64-bit block also consider asweak.AES was to be used128-bit block with128-bit keys. Rijendeal was founder. In this drop we are using it to encrypt the data owner file.
Input:
128_bit /192 bit/256 bit input (0, 1)
Secret key (128_bit) +plain text (128_bit).
Process:
10/12/14-rounds for-128_bit /192 bit/256 bit input
Xor state block (i/p)
Final round:10,12,14
Each round consists: sub byte, shift byte, mix columns, add round key.
Output:
cipher text(128 bit)

VI. RESULT

Results 1:
In this subsection, our System evaluates the performance of the proposed scheme by several experiments. System runs these experiments on a window machine with an Intel processor 2.30GHz processor and 8GB memory. All these experiments use Java programming language with the various encryption algorithms such as AES (Proposed system), CP-ABE (Existing System).

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

Graph 1: Shows file size on x axis and Encryption Time on Y-axis

Table 1: Show File Size and Encryption Time

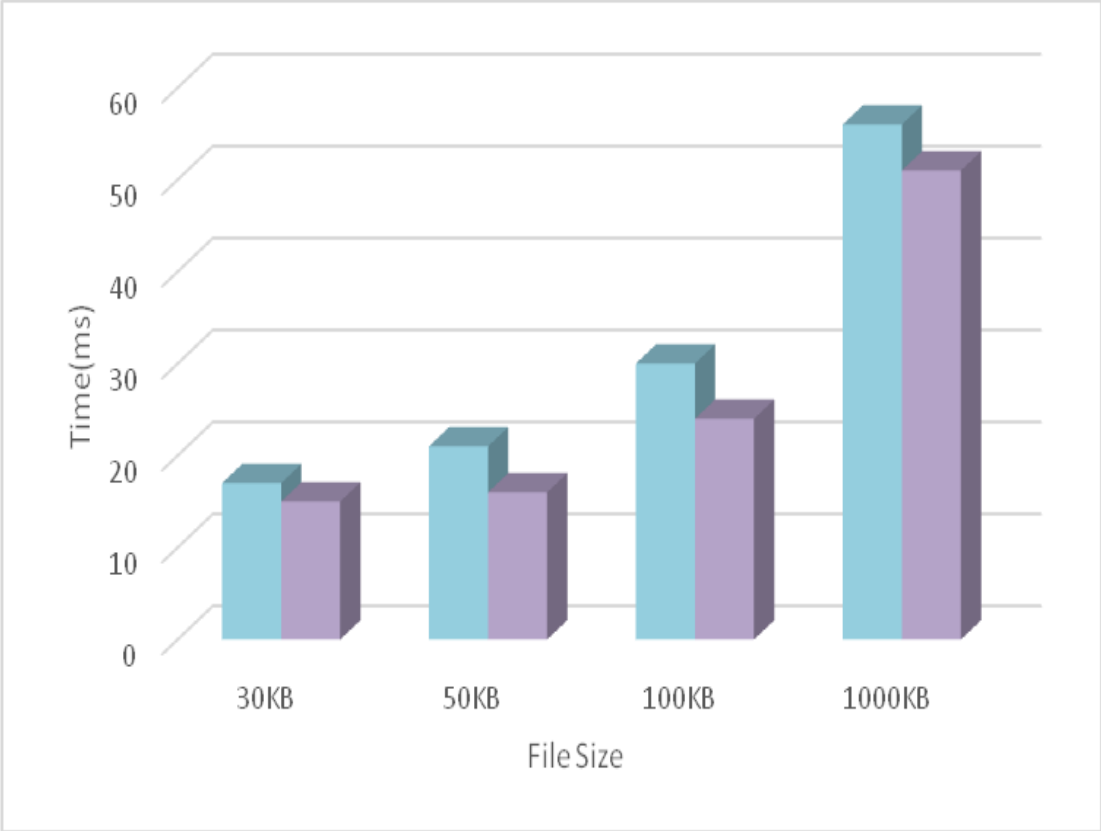
Index Number	Image size (KB)	CP-ABE Encryption Time	AES Encryption Time
1	30	31	28
2	50	36	31
3	100	63	58
4	1000	102	93

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

Results 2:



Graph 2: Shows file size on x axis and Decryption Time on Y-axis

Table 2: Show File Size and Decryption Time

Index Number	Image size (KB)	CP-ABE Decryption Time	AES Decryption Time
1	30	12	9
2	50	16	12
3	100	26	21
4	1000	52	46

VII. CONCLUSION

The proposed system enhances the security of data by encrypting and distributing the data across multiple peers in the system. Implemented system uses the AES 256bit encryption algorithm to encrypt the data ensuring the confidentiality of the user's data. Encrypted data is then distributed and stored across peers in the network using the IPFS protocol. Our system not only solves the privacy and security concerns of centralized cloud storage but also provides a medium for the peer to rent their underutilized storage and earn cryptocurrency in return thereby, maximizing the storage resource utilization.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905174 |

REFERENCES

[1] D. Song, D. Wagner, A. Perrig, "Practical techniques for searches on encrypted data," in: SP'00, Berkeley, CA, 2000.
[2] E. Goh, "Secure indexes," Cryptology ePrint Archive, pp. 216 – 216, 2003.
[3] A. Broder, M. Mitzenmacher, "Network applications of bloom filters: A survey," Internet Math., vol. 1, no. 4, pp. 485 – 509, 2002.
[4] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," Journal of Computer Security, vol. 19, no. 5, pp. 895 – 934, 2011.
[5] Q. Liu, G. Wang, J. Wu, "Secure and privacy preserving keyword searching for cloud storage services," J NETW COMPUT APPL., vol. 35, no. 3, pp. 927 – 933, 2012.
[6] C. Wang, N. Cao, J. Li, K. Ren, W. Lou, "Secure ranked keyword search over encrypted cloud data," in: ICDCS'10, Genoa, Italy, 2010.
[7] C. Liu, L. Zhu, J. Chen, "Efficient searchable symmetric encryption for storing multiple source dynamic social data on cloud," J NETW COMPUT APPL., vol. 86, pp. 3 – 14, 2017.
[8] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," in: INFOCOM'11, Shanghai, China, 2011.
[9] A. Ibrahim, H. Jin, A. Yassin, D. Zou, "Secure rank-ordered search of multi-keyword trapdoor over encrypted cloud data," in: APSCC'12, Guilin, China, 2012.
[10] Z. Shen, J. Shu, W. Xue, "Preferred keyword search over encrypted data in cloud computing," in: IWQoS'13, Montreal, Canada, 2013.
[11] B. Wang, S. Yu, W. Lou, Y. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in: INFOCOM'14, Toronto, Canada, 2014.
[12] S. Pasupuleti, S. Ramalingam, R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," J NETW COMPUT APPL., vol. 64, pp. 12 – 22, 2016.
[13] W. Sun, B. Wang, N. Cao, H. Li, W. Lou, Y. Hou, H. Li, "Privacy preserving multi-keyword text search in the cloud supporting similarity based ranking," IEEE T Parall Distr., vol. 25, no. 11, pp. 3025 – 3035, 2014.
[14] Z. Xia, X. Wang, X. Sun, Q. Wang, "A secure and dynamic multikeyword ranked search scheme over encrypted cloud data," IEEE T Parall Distr., vol. 27, no. 2, pp. 340 – 352, 2016.
[15] C. Dong, G. Russello, N. Dulay, "Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, vol. 19, no. 3, pp. 367 – 397, 2011.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details