IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org
ISSN (e): 2250-3021, ISSN (p): 2278-8719 Special Issue || September 2021 || PP 88-92
7th National Conference On Advancements in Communication, Computing and Electronics Technology-ACCET 2021

Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm

P. N. KOTA
Department of Electronics and Telecommunication
Q. *MES's College of Engineering, Pune, India*

OMKAR K. PINJARE
R. Department of Electronics and Telecommunication
S. *MES's College of Engineering, Pune, India*

SHRADHA K. DIGHE
T. Department of Electronics and Telecommunication
U. *MES's College of Engineering, Pune, India*

Tushar N. Warale
Department of Electronics and Telecommunication
MES's College of Engineering, Pune, India

Abstract: *Recruitment is a function of human resource management by which an organization can attract the potential candidates and select the most appropriate employees for the organization.Now-a-days the people are extensively adaptive to the technology and that's why e-recruitment has become a popular practice followed by the organization for hiring employees. The online recruitment document sharing application that will help in sharing the important documents between the College authority (Administrator) and the Company HR with great ease. The college students will be given the hard copy of their document (resume) that they need to study for the recruitment.*

The analysis between database and file system could have been done better, by uploading, downloading and searching files from a different computer that does not host the web application. Analysis would have also been better if files of bigger size (like 1GB or 2 GB) were uploaded and downloaded.

Keywords: Cloud computing, Hybrid Cryptography

I. INTRODUCTION

The world came to know about the Block-chain concept nine years back when Satoshi Nakamoto conceptualized it in 2008; but it got developed a year later, using Bit-coin, a crypto-currency and digital payment system. The concept was later discovering to distributed ledger that leverages the block-chain to verify and store transactions without crypto-currency. The term block-chain is broadly used these days to represent a new disruptive technology poised to be the next big thing across industries from healthcare to finance to retail. According to Gartner, their client analysis on block-chain and related topics has quadrupled since August 2015.

Block-chain is a divided database of records or public ledger of digital events or transactions that got executed and has been shared among involving parties across a large network of un-trusted participants. It stores data in blocks that can verify information and are very difficult to hack.

A block-chain is a public ledger residing of ordered and time-stamped records of transactions arranged in data blocks which will use cryptographic validation to link themselves together. Block-chain is a path of recording data and transactions digitally. Each record is a block connected chronologically together into a chain. A block of one or more new transactions is composed into the transaction data part of a block. According to the approach of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, usually appended to the data file.

Block chain is touted for its potential to improve the trust and transparency of data- based transactions between individuals and organizations. The technology offers promise when strategically applied in the right contexts. But what are the conditions under which block chain makes sense and how might the technology be useful when applied in government? Traditionally, organizations operating their own, individual IT systems seeking to collaborate must reckon with challenges including reconciliation of information, identifying a single source of truth, and facilitating accountability.

Block chain technology addresses these challenges by providing a technical foundation that supports the execution of shared business processes in a way that no single entity controls the entire system. Government has an inherent need to build, sustain, and protect public trust in information and systems. In some situations, block chain may help enhance this trust. Traditional relational database management solutions (e.g. Oracle and SQL), deployed globally across millions of applications, have one major operational constraint – the management of data is performed by a few entities who must be trusted. Distributed Ledger Technologies (DLT, commonly referred to as block chain), an alternative architectural approach to managing data, and removes the need for a trusted authority to store and share a perpetually growing set of data. A foundational characteristic of a block chain is trust.

Block chain have digital signatures and use keys to authorize and check transactions and positively identify the initiator. Once recorded to the chain, a block chain record cannot be deleted or manipulated. New blocks may only be appended to the chain, ensuring data integrity and creating a verifiable audit trail where the shared ledger provides visibility to all participants, simultaneously. Additionally, data elements can be individually permissioned, so participants see only appropriate transactions. Applications managed by a single entity would typically not benefit from using block chain technology.

As the name connotes, block chain is a chain of blocks. Each block represents a record or set of data, that is linked to others with cryptography. Each block contains some accessible information to provide public knowledge about the action, time, or some other feature of the record, creating a public transcript of how the information develops, known as a “ledger.” As transactions enter a block chain system, a consensus model is employed to determine which next set of valid transactions, or block, should be appended to the ledger. Because consensus is established over a distributed network for nodes, there is no central authority that governs the validation and inclusion of new transaction data. As most block chain software is open source, the rules that adjudicate the blocks and included transaction data are available for review. For public block chain systems, the data itself is available for direct observation by anyone who cares to access it. This makes open block chain datasets perceived of as more reliable to a greater number of users.

II. METHODOLGY

A. System Design: -

System Architecture

Analysis of Input and expected Output Related to Project

Input: Original file

Output: 1. Encrypted file

1. Unreadable Format
2. Generate Private key
3. Distributed data

UML Diagrams

UML stands for Unified Modelling Language. It is a standard visual modelling language in the field of software engineering. It provides the standard way to visualize the design of a system

Use-Case Diagram

A use case diagram is a graphic depiction of the interactions among the elements of a system. A use case is a methodology used in system analysis to identify, clarify, and organize system requirements. The relationships between and among the actors and the use cases.

A use case illustrates a unit of functionality provided by the system. The main purpose of the use- case diagram is to help development teams visualize the functional requirements of a system, including the relationship of "actors" to essential processes, as well as the relationships among different use cases. Use-case diagrams generally

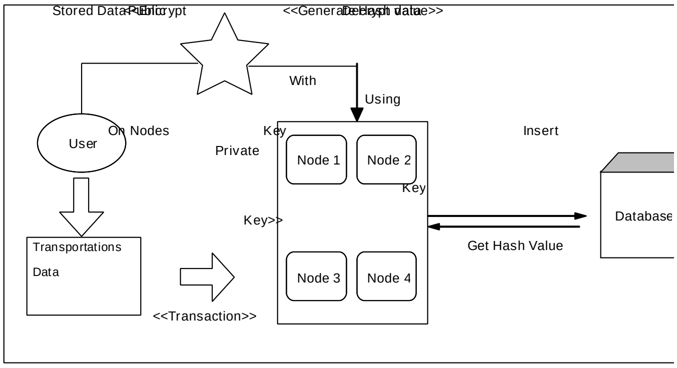

Figure 1: system Architecture

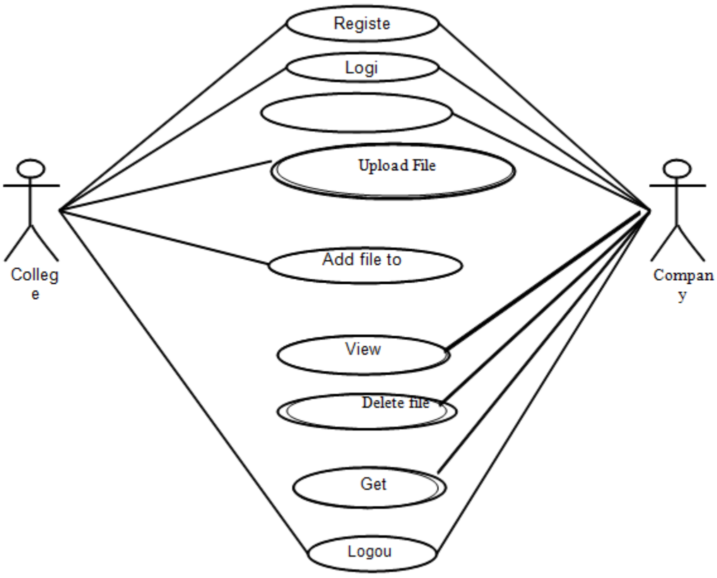

Figure 2: Use-Case Diagram

show groups of use cases, either all use cases for the complete system, or a breakout of a particular group of use cases with related functionality to Show a use case on a use-case diagram, you draw an oval in the middle of the diagram and put the name of the use case in the centre of, or below, the oval. To draw an actor (indicating a system user) on a use-case diagram, you draw a stick person to the left or right of your diagram. Following diagram shows the relationships of the user or actors with the use cases which are shown in an oval shape.

B. Activity Diagram

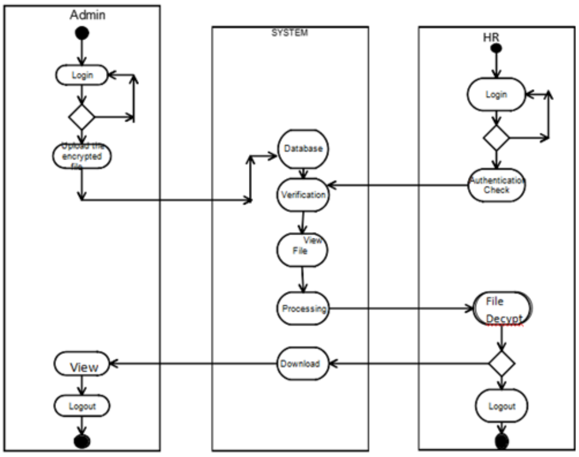

Figure 3: Activity Diagram

An activity diagram is a behavioural diagram i.e. it depicts the behaviour of a system. An activity diagram portrays the control flow from a start point to a finish point showing the various decision paths that exist while the activity is being executed.

III. ER DIAGRAM

An entity-relationship diagram (ERD) is a data modelling technique that graphically illustrates an information system's entities and the relationships between those entities. An ERD is a conceptual and representational model of data used to represent the entity framework infrastructure.

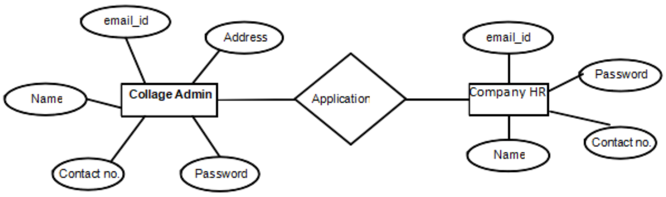

Figure 4: Entity Relation Diagram

A. State Diagram

A state diagram is a type of diagram used in computer science and related fields to describe the behaviour of systems. State diagrams require that the system described is composed of a finite number of states.

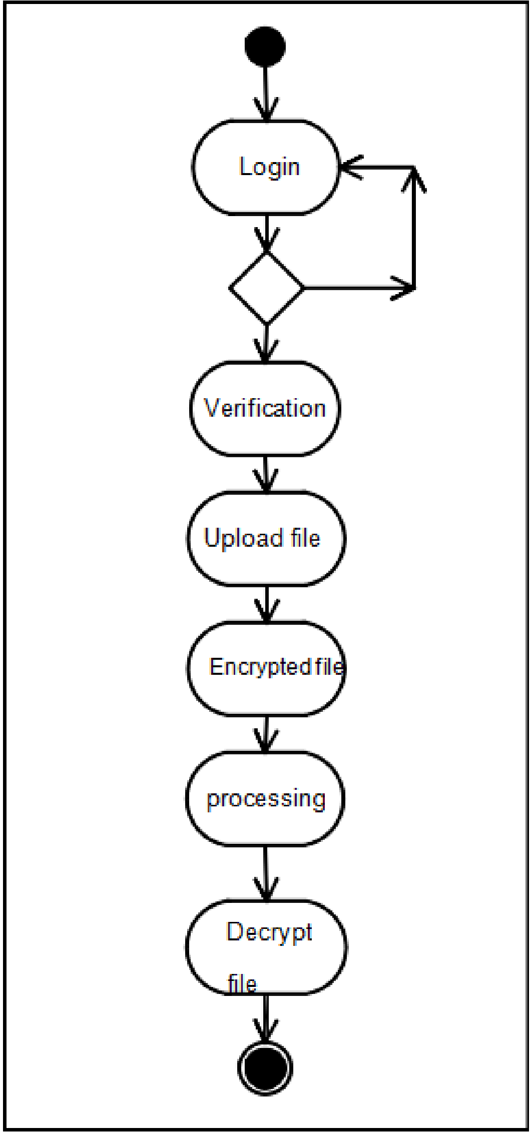

Figure 5. State Diagram

IV. CONCLUSION

In work is designed using block chain concept and key-based cryptographic technique which estimate the security of block-chains specifically using hashing. Proposed system work to security on transportation data.Block-chain technology is not just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes. This approach allows users to authenticate the data access through the public and private key of user sources, while improving network access performance by locally authenticating keys based on block-chain copies and its hash values. This work is designed using block chain concept and key-based cryptographic technology to provide the security to transportation data of vehicle and product.

REFERENCES

[1]. R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," *IEEEIntell. Transp. Syst. Mag.*, vol. 8, no., pp. 33–44, Fall 2016.

[2]. Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3]. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[4]. N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Comput.

[5]. M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in *Proc. IEEE 11the Int. Conf. Eur. Energy Market*, 2014, pp. 1–6.

[6]. S. Barber *et al*, "Bitter to better-how to make bitcoin a better currency," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2012, pp. 399–414.

[7]. I. Alqassem *et al.*, "Towards reference architecture for cryptocurrencies: Bitcoin architectural analysis," in *Proc. IEEE Internet Things, IEEE Int.Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput.* 2014, pp. 436–443.

[8]. K. Croman *et al.*, "On scaling decentralized blockchains," in *Proc. Int. Conf. Financial Cryptography Data Security*, 2016, pp. 106–125.

[9]. G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Banking Beyond Banks andMoney*. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[10]. L. Luu *et al.*, "A secure sharding protocol for open blockchains," *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2016, pp. 17–30.