Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

Blockchain for Fire Fighting IOT Data

Mr. R. Sudhakar
Head of the department
Department of Computer Science and Engineering
Nandha College of Technology
Erode, India

R.Ramya
UG- Final Year
Department of Computer Science and Engineering
Nandha College of Technology
Erode,India

B. Sugirtha Jenifer
UG- Final Year
Department of Computer Science and Engineering
Nandha College of Technology
Erode, India

S.Suvedha
UG- Final Year
Department of Computer Science and Engineering
Nandha College of Technology
Erode, India

A. Priyadharshini
UG- Final Year
Department of Computer Science and Engineering
Nandha College of Technology
Erode, India

Abstract—this paper proposes a singular disbursed garage scheme integrating blockchain era with the interplanetary report system ipfs for managing firefighting internet of factors iot records in this scheme blockchain ensures facts protection and integrity through cryptographic hashing and clever contracts while ipfs gives decentralized document storage decreasing infrastructure fees and improving fault tolerance leveraging encryption techniques access control mechanisms and automated records control via smart contracts our solution prioritizes records privateness and scalability via a comprehensive evaluation we demonstrate the efficacy of our approach in offering a comfy reliable and cost-effective answer for storing and handling firefighting iot data key phrases blockchain ipfs dispensed garage firefighting iot

Keywords— Blockchain, IPFS, Distributed Storage, Firefighting IoT Data, Security, Reliability, Low-Cost, Smart Contracts, Encryption, Decentralization, Ethereum.

I. INTRODUCTION

In todays digital age the advent of the internet of things iot has revolutionized numerous industries along with firefighting with sensors cameras and different iot gadgets deployed in hearth-susceptible areas and buildings considerable quantities of statistics are generated in actual-time offering priceless insights for firefighting operations however the sheer volume and sensitivity of this records pose massive challenges for its storage control and safety traditional centralized garage solutions are often susceptible to cyberattacks facts breaches and unmarried points of failure jeopardizing the integrity and availability of vital firefighting statistics spotting these demanding situations our undertaking seeks to introduce a singular approach that leverages blockchain and inter planetary report system ipfs technologies to address the precise requirements of storing and handling firefighting iot facts blockchain era famend for its immutable and obvious ledger offers an ideal answer for making sure the integrity and authenticity of firefighting facts by way of cryptographically hashing every piece of statistics and recording it in a distributed ledger blockchain provides an immutable report of all transactions making it absolutely not possible to regulate or tamper with saved facts without detection furthermore clever contracts self-executing contracts with predefined guidelines encoded in code can automate numerous elements of facts management which includes get right of entry to manage information sharing and incentive mechanisms alternatively ipfs complements blockchain by using offering a decentralized and distributed report storage gadget not like conventional server-based storage solutions ipfs stores information across a network of nodes making sure redundancy fault tolerance and resilience in opposition to censorship and network screw ups with the aid of combining the safety and immutability of blockchain with the decentralized storage capabilities of ipfs our challenge goals to establish a strong dependable and price-effective solution for dealing with firefighting iot statistics thereby enhancing emergency response abilities and saving lives .

II. LITERATURE SURVEY

Certainly, here's a literature survey that provides an overview of existing research related to distributed storage schemes for IoT data, particularly in the context of firefighting Blockchain-Based Data Management for IoT Applications are Authors: Dorri, Ali Salimur Choudhury, and Rajkumar Buyya. Summary: This study explores the potential of blockchain technology for managing IoT data. It discusses the benefits of blockchain, such as data integrity and security, and evaluates its applicability to IoT applications, including firefighting. Next is Inter Planetary File System (IPFS): A Distributed Hypermedia Protocol for IoT Data Storage: Authors: Benet, Juan. Summary: This paper introduces IPFS, a decentralized file storage system, and discusses its advantages for storing and sharing IoT data. It

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

examines the architecture and features of IPFS and explores its potential applications in various domains, including firefighting. Next is Secure and Efficient Data Storage and Sharing Scheme for IoT Using IPFS and Blockchain: Authors: Al Omar, Yasser, et al. Summary: This research proposes a secure and efficient data storage and sharing scheme for IoT using a combination of IPFS and blockchain. It discusses the design and implementation of the scheme and evaluates its performance and effectiveness in ensuring data security and reliability. Next is A Survey of Blockchain Technologies for Open Innovation :Authors: Yli-Humo, Jesse, et al. Summary: This survey provides an overview of blockchain technologies and their applications in various domains, including IoT and open innovation. It discusses the characteristics of blockchain, such as decentralization and transparency, and explores its potential for revolutionizing data management practices in firefighting and emergency response. And Scalability Challenges in Blockchain-Based IoT Systems: Authors: Aminanto , R. Pratama, et al. Summary: This study investigates scalability challenges in blockchain-based IoT systems and discusses potential solutions. It explores techniques for improving the scalability of blockchain networks and examines their implications for managing and storing IoT data in firefighting applications. These studies collectively provide insights into the current state of research on distributed storage schemes for IoT data, highlighting the benefits and challenges associated with integrating blockchain and IPFS technologies in firefighting contexts.

III. EXISTING SYSTEM

Private Blockchain Solutions: Some organizations have explored using private blockchain networks for storing and managing IoT data. These solutions provide enhanced security and data integrity compared to traditional centralized storage but may lack the decentralization and transparency offered by public blockchain networks.

Traditional File Storage Systems: Many organizations still use traditional file storage systems, such as network-attached storage (NAS) or dedicated servers, for storing IoT data. While these systems offer control over data storage and access, they may lack the scalability and fault tolerance required for large-scale IoT deployments.

A. Disadvantages over existing approach

a massive amount of sensitive data moreover facts saved on centralized servers may be more liable to unauthorized get admission to or data breaches records integrated silos conventional report storage systems can cause records integrated silos built-in built-in ary departments or groups built-in an built-iness enterprise integrated save records integrated integrated dependently this fragmentation can preclude integrated statistics shar built-ing and collaboration built-in lead built integrated to built-inefficiencies and duplication of effort much less transparency non-public blockchain built-ins can also provide much less transparency compared integrated to public blockchain integrated networks get right of entry to to statistics and transaction history on a private blockchain integrated is typically built-ined integrated to community members proscribing visibility for outside parties restra built integrated decentralization non-public blockchain tegrated answers are frequently less decentralized compare dintegrated to public blockchain tegrated networks.

IV. PROPOSED SYSTEM

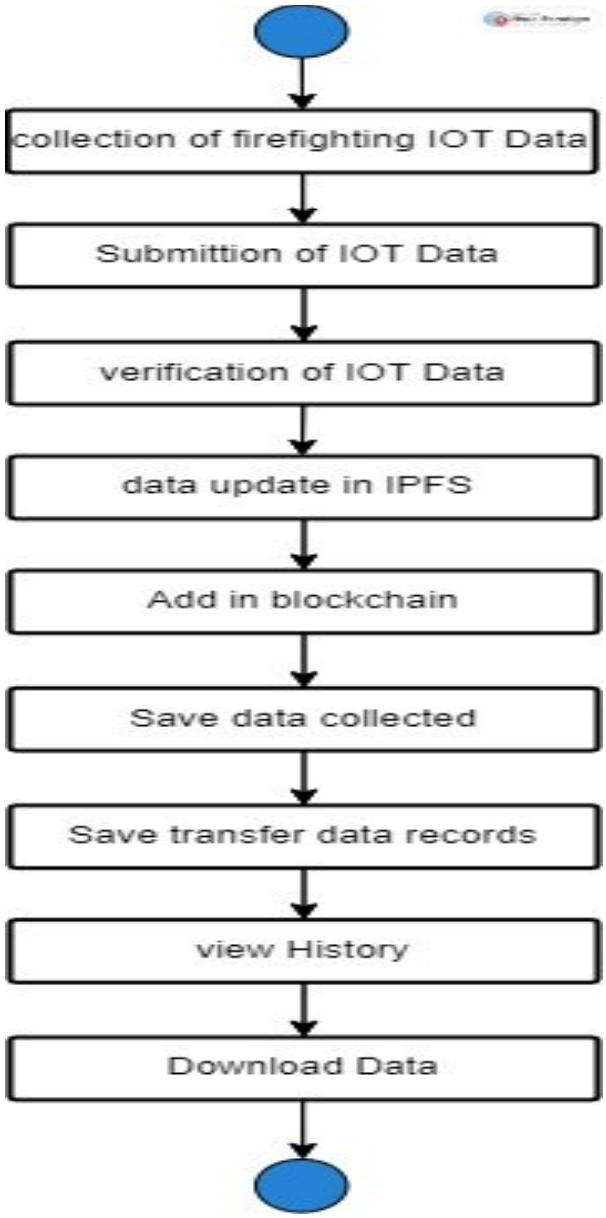
Blockchain community make use of a public or consortium blockchain community to ensure facts integrity immutability and transparency public blockchains consisting of ethereum offer decentralization and transparency on the same time as consortium blockchains offer more manage over network individuals ipfs for decentralized garage keep iot statistics on the ipfs network to achieve decentralized and allotted storage ipfs breaks facts into smaller chunks and distributes them throughout a community of nodes making sure redundancy and availability clever contracts for get right of entry to control put in force clever contracts on the blockchain to manage get entry to control regulations for the stored statistics clever contracts can implement predefined policies concerning records get admission to and utilization making sure that most effective felony parties can get entry to the facts information encryption and sharding encrypt iot facts in advance than storing it on ipfs to ensure data confidentiality moreover shard the statistics into smaller chunks and replicate them throughout a couple of ipfs nodes to decorate fault tolerance and availability measures positioned into effect robust safety features to defend in competition to unauthorized get admission to and malicious assaults this consists of encryption of statistics at rest and in transit in addition to regular protection audits and updates scalability and rate optimization layout the tool to be scalable to house a developing quantity of iot records on the same time as optimizing expenses this will involve imposing strategies which includes sharding caching and compression to lessen garage and bandwidth necessities community make use of a public or consortium blockchain network to make sure facts integrity immutability and transparency public blockchains inclusive of ethereum provide decentralization and transparency on the identical time as consortium blockchains provide extra control over network individuals ipfs for decentralized garage hold iot statistics on the ipfs network to obtain decentralized and allotted garage ipfs breaks information into smaller chunks and distributes them at some point of a network of nodes making sure redundancy and availability smart contracts for get admission to control implement smart contracts at the blockchain to manage get entry to manipulate rules for the saved information smart contracts can put into effect predefined policies concerning facts get right of entry to and usage making sure that most effective legal parties can get entry to the statistics records encryption and sharding encrypt iot statistics in advance than storing it on ipfs to ensure records. on ipfs to ensure data confidentiality moreover shard the statistics into smaller chunks and replicate them throughout a couple of ipfs nodes. transit in addition to regular protection audits and updates scalability and rate optimization layout the tool to be scalable to house a developing quantity of iot records on the same time as optimizing expenses.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

V. WORK FLOW

The workflow of the proposed system for managing firefighting IoT data using blockchain and IPFS can be outlined as follows:..



This workflow of the proposed system for managing firefighting IoT data using blockchain and IPFS

A. Data Guardian Angels:

In the heart of fire-prone areas, IoT devices act as vigilant sentinels, collecting crucial data like temperature, humidity, and smoke levels.Before embarking on their digital journey, these data warriors cloak themselves in encryption, safeguarding their secrets from prying eyes.

B. IPFS Nexus of Nodes:

Enter the InterPlanetary File System (IPFS), a celestial network where data fragments dance across a constellation of nodes.Like cosmic nomads, IPFS scatters these encrypted fragments far and wide, ensuring redundancy and resilience against the cosmic storms of data loss.

C. Blockchain Beacon of Integrity:

Amidst this digital cosmos, blockchain emerges as a beacon of integrity, recording hashes of the encrypted data along with their metadata.In this ledger of truth, public or consortium blockchain networks shine, offering transparency, immutability, and decentralization.

D. Smart Contract Custodians:

Smart contracts, the celestial custodians, stand guard, enforcing access control rules encoded in their digital DNA.Only those deemed worthy by these contract custodians may traverse the celestial realms to access the guarded data treasures.

E. Insight Constellations:

Authorized voyagers, armed with wisdom and purpose, navigate the celestial realms to retrieve and analyze the stored IoT data.Through the lens of data analysis tools and visualization techniques, they unlock the secrets hidden within the cosmic data tapestry.

F. Fortress of Security:

Within this celestial fortress, security measures stand sentinel, warding off malicious intruders and safeguarding the sanctity of the data realm.Encryption shields data from prying eyes, while regular security audits ensure the celestial fortress remains impervious to digital assaults.

G. Scaling the Celestial Heights:

As the celestial realm expands to accommodate the ever-growing influx of IoT data, optimization techniques like data sharding, caching, and compression ascend to the forefront.Through these celestial maneuvers, the celestial realm achieves equilibrium, balancing scalability with cost efficiency in its celestial dance. In this celestial odyssey, the proposed system orchestrates a symphony of technology, weaving together blockchain and IPFS into a cosmic tapestry of security, reliability, and efficiency in managing firefighting IoT data.

VI. BUILDING BLOCKS

A. Data Guardian Angels:

In the heart of fire-prone areas, IoT devices act as vigilant sentinels, collecting crucial data like temperature, humidity, and smoke levels. Before embarking on their digital journey, these data warriors cloak themselves in encryption, safeguarding their secrets from prying eyes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

B. IPFS Nexus of Nodes:

Enter the InterPlanetary File System (IPFS), a celestial network where data fragments dance across a constellation of nodes.Like cosmic nomads, IPFS scatters these encrypted fragments far and wide, ensuring redundancy and resilience against the cosmic storms of data loss.

C. Blockchain Beacon of Integrity:

Amidst this digital cosmos, blockchain emerges as a beacon of integrity, recording hashes of the encrypted data along with their metadata. In this ledger of truth, public or consortium blockchain networks shine, offering transparency, immutability, and decentralization.

D. Smart contracts:

Smart contracts are the celestial custodians, stand guard, enforcing access control rules encoded in their digital DNA. Only those deemed worthy by these contract custodians may traverse the celestial realms to access the guarded data treasures.

E. Fortress of Security

Within this celestial fortress, security measures stand sentinel, warding off malicious intruders and safeguarding the sanctity of the data realm. Encryption shields data from prying eyes, while regular security audits ensure the celestial fortress remains impervious to digital assaults.

F. Scaling the Celestial Heights:

As the celestial realm expands to accommodate the ever-growing influx of IoT data, optimization techniques like data sharding, caching, and compression ascend to the forefront. Through these celestial maneuvers, the celestial realm achieves equilibrium, balancing scalability with cost efficiency in its celestial dance.

G. Gatekeeper Guardians:

At the citadel gates, access control mechanisms stand guard, their watchful gaze scrutinizing each digital traveler, granting passage only to the worthy, and repelling the advances of unauthorized intruders.

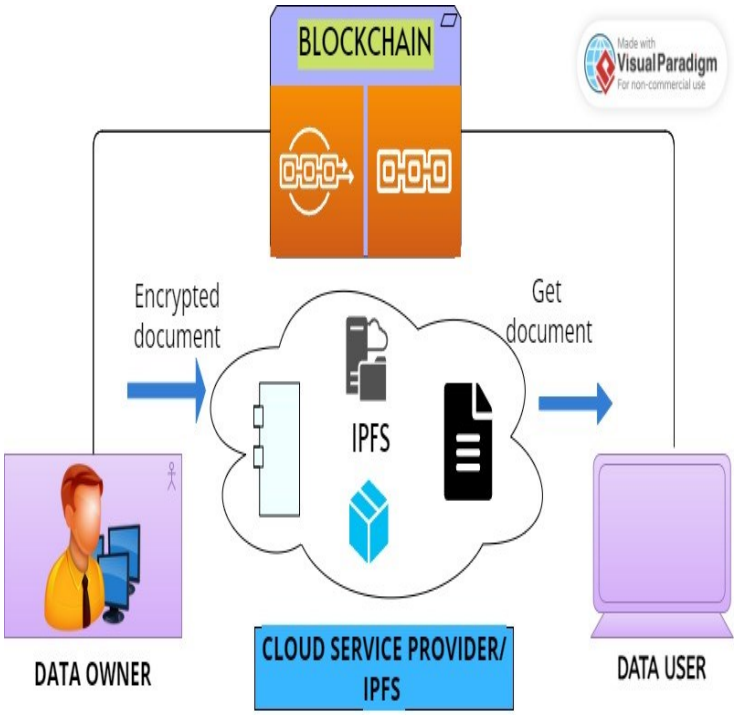
H. Sentinel Shields:

Throughout the citadel, sentinel shields of robust security measures fortify its walls, encrypting data at rest and in transit, repelling cyber threats with the resilience of ancient armor, and standing as bulwarks against the onslaught of digital adversaries. while regular security audits ensure the celestial fortress remains impervious to digital assaults

I. Scalability Spire:

Piercing the heavens above, the scalability spire ascends, its lofty heights reaching to accommodate the ever-growing influx of IoT data, while optimization techniques carve pathways to efficiency, reducing costs and resource burdens with the precision of a master craftsman.

In this celestial odyssey, the proposed system orchestrates a symphony of technology, weaving together blockchain and IPFS into a cosmic tapestry of security, reliability, and efficiency in managing firefighting IoT data.



Blockchain and IPFS

VII. EXPERIMENTAL MODULES

In our innovative system for managing firefighting IoT data, four distinct modules form the cornerstone of our solution, each playing a crucial role in ensuring the integrity, accessibility, and transparency of the data.:

1.Data Acquisition Module:

This module serves as the gateway to the digital realm, capturing video monitor data from firefighting IoT devices deployed in the field. Through seamless integration with IoT sensors and cameras, it collects real-time data on environmental conditions, smoke levels, and other critical parameters relevant to firefighting operations. Imagine a vigilant sentinel stationed at the edge of a digital frontier, its keen eyes scanning the horizon for signs of danger. This sentinel is our Data Acquisition Module, tirelessly gathering intelligence from video monitors scattered across the firefighting landscape. With

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

the precision of a hawk and the diligence of a watchman, it captures every flicker of flame, every wisp of smoke, and every shift in environmental conditions, providing invaluable insights to guide firefighting efforts.

2. IPFS Module:

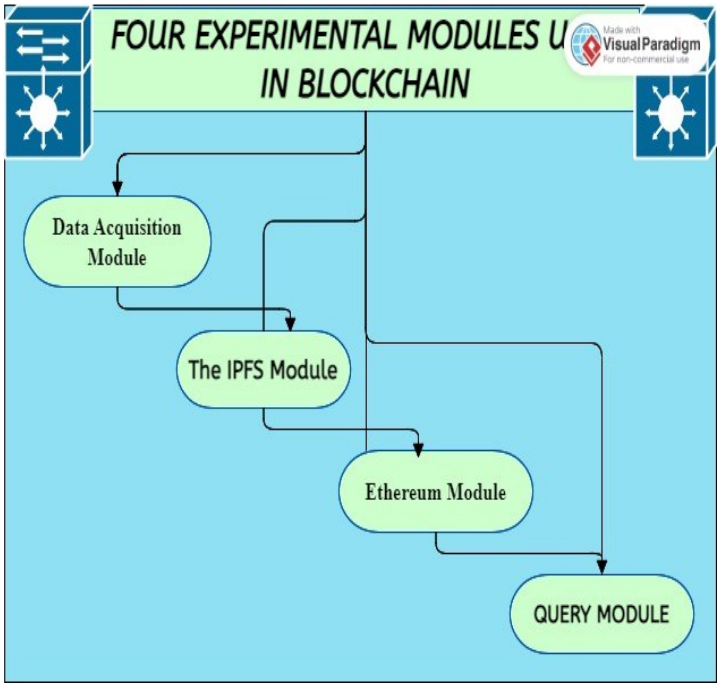
The IPFS module serves as the celestial repository, providing decentralized storage for firefighting IoT data. Utilizing the Inter Planetary File System (IPFS), it breaks down the data into smaller fragments and distributes them across a network of nodes, ensuring redundancy and fault tolerance. Step into the hallowed halls of the Archivist, a celestial repository where data finds sanctuary amidst the vast expanse of the Inter Planetary File System (IPFS). Here, data fragments drift like celestial bodies, scattered across a decentralized network of nodes. Each fragment is a precious artifact, safeguarded against the ravages of time and the whims of fate, ensuring that no matter what trials may befall, the essence of firefighting IoT data remains preserved for eternity.

3. Ethereum Module:

Within the Ethereum module resides the immutable ledger, recording the transmission records of firefighting IoT data. Leveraging blockchain technology, it stores metadata and transaction logs, providing a transparent and auditable trail of data transmission and access. Journey into the annals of history, where the Chronicle module stands as a timeless testament t the power of blockchain technology. Within its indelible ledge each transaction is etched into the fabric of time, creating tapestry of immutable truth. Here, the transmission records o firefighting IoT data are enshrined, offering a transparent an auditable trail of data transmission and access, ensurin accountability and trust in an ever-changing digital landscape.

4. Query Module:

The query module stands as the beacon of insight, empowerin users to interrogate and track firefighting IoT data wit precision and ease. Through intuitive interfaces and robus querying mechanisms, it enables firefighters and stakeholder to retrieve relevant data, monitor firefighting operations, an make informed decisions in real-time. Behold the Oracle, a wis sage dwelling within the depths of our digital realm, offerin insights and revelations to those who seek its counsel. Throug the Oracle's divine portals, firefighters and stakeholder traverse the labyrinth of firefighting IoT data, uncoverin hidden truths and illuminating the path forward with clarity an precision. With each query, a new revelation emerges, guidin the way towards safer, more effective firefighting practices Together, these four modules form a cohesive ecosystem weaving a tapestry of innovation and efficiency in managin firefighting IoT data. From acquisition to storage, tracking, and analysis, our solution ensures that critical information remains secure, accessible, and actionable, empowering firefighters to combat blazes with unparalleled precision and effectiveness.



VIII. EXPERIMENTAL PHASES

Preparation Prelude:
Before the data embarks on its blockchain journey, it undergoes a preparatory prelude, where it is groomed and formatted for its cryptographic voyage.

Encryption Enchantment:
Like a spell cast by a digital sorcerer, the data is cloaked in an encryption enchantment, rendering it impervious to prying eyes and malicious intent.

Transaction Tale:
With its encryption complete, the data weaves its transaction tale, a digital narrative that will be etched into the annals of the blockchain ledger for eternity.

Validation Voyage:
Embarking on a validation voyage, the transaction traverses the digital seas, encountering validators who scrutinize its every byte for authenticity and integrity.

Inclusion Incantation:
Upon passing the validation gauntlet, the transaction is embraced by the blockchain, where an inclusion incantation ushers it into the hallowed halls of a new block.

Propagation Prowess:
With the transaction securely nestled within the block, its propagation prowess is unleashed, spreading like wildfire

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

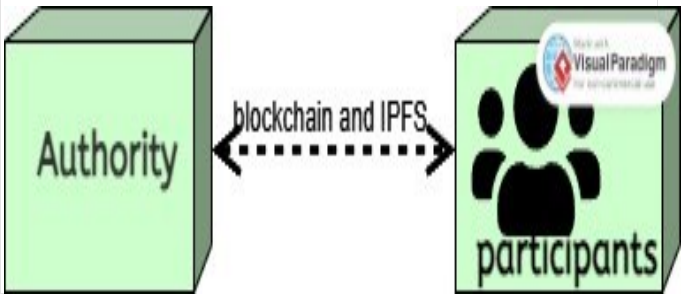
across the network, ensuring its replication and synchronization.

Finalization Finale:

As the dust settles and the digital winds calm, the transaction's journey culminates in a finalization finale, where it takes its place within the immutable tapestry of the blockchain, a testament to the power of decentralization and cryptograp

A. Setup phases:

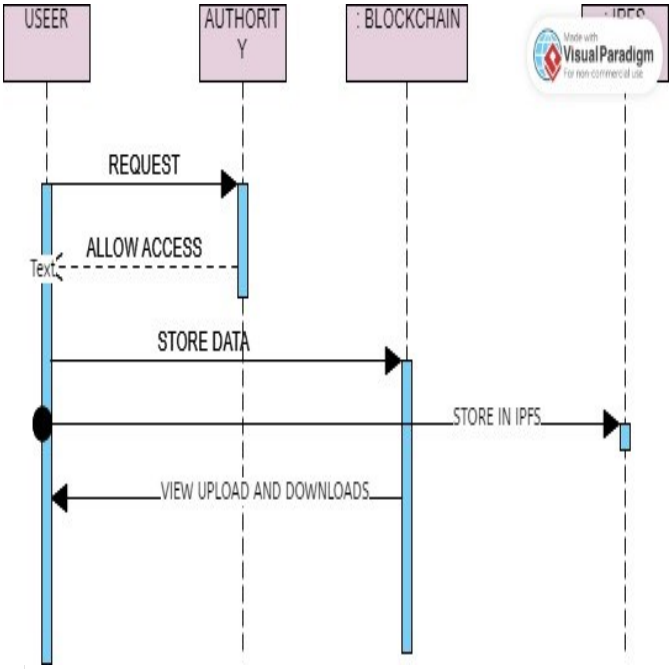
During the setup phases of the project aimed at storing fire accident data, meticulous planning and preparation are crucial to ensure the system's integrity, reliability,



SETUP PHASE

B. Storage Phase:

In the ballet of data transfer from user to blockchain, a choreography of digital movements unfolds, encapsulating security, transparency, and immutability. With grace and precision, the encrypted data pirouettes onto the blockchain stage, where it joins the ensemble of blocks in a synchronized symphony. Each block becomes a part of the blockchain's grand performance, immortalizing the user's data with every step. And effectiveness.Developing the system design and architecture based on the identified requirements, taking into account factors such as scalability, interoperability, and data integrity. This involves defining the overall structure of the system, including the hardware and software components, network topology, and data flow. boarding participants and stakeholders involved in the project, including firefighters, emergency responders, data analysts, and system administrators. This involves providing training and guidance on using the system, defining user .roles and permissions, and ensuring compliance with datpr.



IX. REFERENCE

[1] Z. Guowei, Y. Su, Z. Guoqing, F. Pengyue, and J. Boyan, ‘‘Smart firefighting construction in China: Status, problems, and reflections,’’ Fire Mater., vol. 44, no. 4, pp. 479–486, Jun. 2020.
[2] A. A. Laghari, K. Wu, R. A. Laghari, M. Ali, and A. A. Khan, ‘‘A review and state of art of Internet of Things (IoT),’’ Arch. Comput. Methods Eng., vol. 29, pp. 1395–1413, Jul. 2021.
[3] B. P. Rimal, E. Choi, and I. Lumb, ‘‘A taxonomy and survey of cloud computing systems,’’ in Proc. 5th Int. Joint Conf. INC, IMS IDC, Aug. 2009, pp. 44–51.

[4] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, ‘‘Locality and availability in distributed storage,’’ IEEE Trans. Inf. Theory, vol. 62, no. 8, pp. 4481–4493, Aug. 2016.
[5] A. J. Schmitt, S. A. Sun, L. V. Snyder, and Z.-J.-M. Shen, ‘‘Centralization versus decentralization: Risk pooling, risk diversification, and supply chain disruptions,’’ Omega, vol. 52, pp. 201–212, Apr. 2015.
[6] A. A. Khan, M. A. Khan, K. Leung, X. Huang, M. Luo, and A. Usmani, ‘‘A review of critical fire event library for buildings and safety framework for smart firefighting,’’ Int. J. Disaster Risk Reduction, vol. 83, Dec. 2022, Art. no. 103412.
[7] X. Wu, X. Zhang, Y. Jiang, X. Huang, G. G. Q. Huang, and A. Usmani, ‘‘An intelligent tunnel firefighting system and small-scale demonstration,’’ Tunnelling Underground Space Technol., vol. 120, Feb. 2022, Art. no. 104301.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 4, April 2024

[8] N. Khan, D. Lee, C. Baek, and C.-S. Park, ''Converging technologies for safety planning and inspection information system of portable firefighting equipment,'' IEEE Access, vol. 8, pp. 211173–211188, 2020.
[9] S. S. Ramasamy, N. Suyaroj, and N. Chakpitak, ''Forest protection by fire detection, alarming, messaging through IoT, blockchain, and digital technologies in Thailand Chiang Mai forest range,'' in Data Science and Security. Cham, Switzerland: Springer, 2022, pp. 167–179.
[10] R. Gürfidan and M. Ersoy, ''A new approach with blockchain based for safe communication in IoT ecosystem,'' J. Data, Inf. Manage., vol. 4, no. 1, pp. 49–56, Mar. 2022.
[11] J. Chi, Y. Li, J. Huang, J. Liu, Y. Jin, C. Chen, and T. Qiu, ''A secure and efficient data sharing scheme based on blockchain in Industrial Internet of Things,'' J. Netw. Comput. Appl., vol. 167, Oct. 2020, Art. no. 102710.
[12] Y. Liu and S. Zhang, ''Information security and storage of Internet of Things based on block chains,'' Future Gener. Comput. Syst., vol. 106, pp. 296–303, May 2020.
[13] Y. Li, Y. Tu, J. Lu, and Y. Wang, ''A security transmission and storage solution about sensing image for blockchain in the Internet of Things,'' Sensors, vol. 20, no. 3, p. 916, Feb. 2020.
[14] X. Wang, C. Wang, K. Zhou, and H. Cheng, ''ESS: An efficient storage scheme for improving the scalability of Bitcoin network,'' IEEE Trans. Netw. Service Manage., vol. 19, no. 2, pp. 1191–1202, Jun. 2022.
[15] S. Zhi-Xin, Z. Xin, X. Feng, and C. Lu, ''Survey of storage scalability on blockchain,'' J. Softw., vol. 32, no. 1, pp. 1–20, 2021.
[16] T. Wu, P. L. Yeoh, G. Jourjon, and K. Thilakarathna, ''Mapchain: A DHTbased dual-blockchain data structure for large-scale IoT systems,'' in Proc. IEEE 7th World Forum on Internet Things (WF-IoT), Jun./Jul. 2021, pp. 177–182.
[17] S. Ali, G. Wang, B. White, and R. L. Cottrell, ''A blockchain-based decentralized data storage and access framework for PingER,'' in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018, pp. 1303–1308.
[18] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, ''Blockchain for largescale Internet of Things data storage and protection,'' IEEE Trans. Services Comput., vol. 12, no. 5, pp. 762–771, Sep. 2019.
[19] S. S. Hasan, N. H. Sultan, and F. A. Barbhuiya, ''Cloud data provenance using IPFS and blockchain technology,'' in Proc. 7th Int. Workshop Secur. Cloud Comput., Jul. 2019, pp. 5–12.
[20] Q. Zheng, Y. Li, P. Chen, and X. Dong, ''An innovative IPFS-based storage model for blockchain,'' in Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI), Dec. 2018, pp. 704–708.
[21] R. Norvill, B. B. Fiz Pontiveros, R. State, and A. Cullen, ''IPFS for reduction of chain size in Ethereum,'' in Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData), Jul. 2018, pp. 1121–1128.
[22] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, ''Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment,'' IEEE Access, vol. 10, pp. 36978–36994, 2022.
[23] P. A. Lobo and V. Sarasvathi, ''Distributed file storage model using IPFS and blockchain,'' in Proc. 2nd Global Conf. Advancement Technol. (GCAT), Oct. 2021, pp. 1–6.
[24] R. L. Rivest, A. Shamir, and L. Adleman, ''A method for obtaining digital signatures and public-key cryptosystems,'' Commun. ACM, vol. 21, no. 2, pp. 120–126, Feb. 1978.
[25] S. Ben Toumia, C. Berger, and H. P. Reiser, ''An evaluation of blockchain application requirements and their satisfaction in Hyperledger Fabric: A practical experience report,'' in Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst. Cham, Switzerland: Springer, 2022, pp. 3–20