E-GOVGUARD (EGG): A GOVERNMENT INFRASTRUCTURE USING BLOCKCHAIN

Prof. Abhishek Nachankar[1], Alfiya Khan[2], Khushboo Uike[3], Niyati Harne[4], Shruti Chaurasiya[5], Snehal Lambade[6], Tanushri Masram[7]

[1]Assiatant Professor, Department Of Computer Science & Engineering, KDK College Of Engineering, Nagpur, India.

[2,3,4,5,6,7]Students, Department Of Computer Science & Engineering, KDK College Of Engineering, Nagpur, India.

ABSTRACT

The "eGov Guard (eGG)" project introduces a holistic approach to safeguarding government documents by combining user-friendly web interface, OCR technology, and blockchain-based storage. The resulting system aims to enhance data security, streamline document handling, and boost overall efficiency in government processes. By implementing this solution, governments can significantly improve transparency, reduce fraud risks, and foster public trust.

The project combines HTML, CSS, and JavaScript to provide user interaction and secure access for authorized users. This method involves OCR technology, which extracts important information from documents and digitizes them. Blockchain is known for its immutability and security and is used to store and protect important information. The use of smart contracts on a private blockchain ensures the security of data content and metadata. eGovGuard's key features are to ensure storage and security of work, immutable data that preserves impact, and the use of smart contracts to secure fast transactions.

Keywords: : Blockchain Technology, Data Integrity, Data Organization, E-Government, OCR.

1. INTRODUCTION

As we all currently live in this digital world, where security and transparency matter a lot, our project, eGovGuard, is designed to address the issues of this digital world. eGovernment simplifies online services for us but faces issues like fraud. Our project enhances security and makes it easier to manage our documents. We are creating a user-friendly web app using HTML, CSS, JavaScript, OCR, and the main star of our project, blockchain—smart contracts. eGovGuard, or eGG, represents the essence of our project's mission. Just as an eggshell protects the life within it, eGG aims to be a protective shield for sensitive government documents, preventing tampering, fraud, or any unauthorised access. Our project is more than just technology; it is a safeguard for vital data that aims to enhance transparency, integrity, and trust within the government system. In today's increasingly digital world, where the security and authenticity of government documents are paramount, our project, eGovGuard, serves as a robust solution to address the challenges faced by e-government initiatives. E-government has undoubtedly made online services more accessible and efficient, but it is not without its vulnerabilities, including fraud and document tampering. eGovGuard leverages the power of cutting-edge technologies, specifically blockchain and Optical Character Recognition (OCR), to fortify the integrity and security of government documents. Blockchain, known for its immutability and data integrity, is employed to store and safeguard critical information within government services. This ensures that once data is recorded, it remains unalterable and secure, mitigating the risk of tampering or fraudulent activities. Additionally, our project incorporates a user-friendly login page designed using HTML and CSS, allowing authorized users, such as government employees, to access a secure and transparent document management system. Through this system, users can not only log in securely with their username and password but also securely store and manage their essential documents. Moreover, E-GovGuard enhances transparency and accountability in government processes. Citizens can securely access public records and track the flow of funds, promoting trust and confidence in governmental operations. Smart contracts, self-executing agreements coded onto the blockchain, automate routine tasks, reducing bureaucracy and mitigating the risk of human error.

Blockchain can create a transparent and tamper-proof record of government activities, transactions, and data. This can enhance trust among citizens as they can verify the authenticity of government actions. Blockchain's cryptographic features make it highly secure. Data stored on a blockchain is resistant to tampering and hacking, ensuring the integrity and confidentiality of sensitive government information. These are self-executing contracts with the terms directly written into code. They can automate and enforce agreements between parties, reducing bureaucracy and the potential for disputes. Blockchain can be used for secure identity management systems, providing citizens with control over their personal data while allowing governments to authenticate identities efficiently.

E-Government refers to the use of information technology, particularly the internet, to deliver government services to citizens, businesses, and other government agencies. One aspect of e-Government that's gaining attention is the use of blockchain technology to enhance security, transparency, and efficiency in government operations.

Aim

The aim of the project titled "E-Government Guard: Government Blockchain" is to develop a robust and secure blockchain-based system tailored specifically for e-government applications. The primary objective is to address existing challenges in traditional government service delivery, such as data security vulnerabilities, lack of transparency, and inefficiencies in information management. In the digital age, securing and managing government documents is crucial for transparency and accuracy. Our project, **"**eGov Guard (eGG): Government Blockchain**,"** enhances document security and management. It uses django, OCR, and blockchain – smart contracts.

Purpose

In this system, users provide important details such as invoices or other private information using the userfriendly front-end interface. Data entry as source and Data is stored in a powerful and efficient database This storage located internally facilitates access to information needed for future work and business

2. LITERATURE REVIEW

The field of electronic government (e-government) is gaining prominence in contemporary society, as it has a significant influence on the wider populace within the context of a technologically advanced world. E-government makes use of information and communication technologies (ICTs) at various levels and domains within government agencies and the public sector. ICT reduces manual labor, potential fraud points, errors, and process lapses. The Internet's quick accessibility and the widespread adoption of modern technologies and disciplines, such as big data, the Internet of Things, machine learning, and artificial intelligence, have accelerated the need for e-government. However, these developments raise a number of data reliability and precision concerns. The adoption of blockchain technology by researchers demonstrates its efficacy in addressing such issues. The present study proposes the SEC Hash system model, which integrates blockchain and Optical Character Recognition (OCR) technologies for the purpose of regulating the processing of incoming documents by governmental agencies. As a case study to assess the proposed system paradigm, the study uses a document containing incoming invoices. The proposal seeks to maintain the integrity of document data by prohibiting its modification after acceptance. Additionally, SEC Hash guarantees that accepted documents will not be destroyed or lost. The analysis demonstrates that using the SEC Hash model system will decrease fraudulent transactions by eradicating manual labor and storing documents on a blockchain network. E-government is a method of delivering government services through the use of information and communication technology (ICT) applications. The concept of E government refers to the development of information technology infrastructure within governmental institutions. Thus, facilitating immediate access to public data and enhancing public services. This involves transitioning from an internet-based connection among departments to a more secure private network, ensuring decentralized data collection, storage, and processing. The fundamental objective remains to uphold data integrity and immutability.

The existing system

E-government is when the government uses technology to make things easier for people and businesses. They put information online so you can access it from your computer or phone. This helps save time and money and makes government services better. But there are problems like fraud and mistakes that can happen. To solve these problems, a new system called SECHash (Scanning, Extraction, Confirmation, and Hashing of Documents) uses technology to make sure government documents are genuine and can't be changed or faked. It uses two important things: blockchain and OCR. Blockchain is like a digital lockbox where information is stored in blocks. Once something is put in the lockbox, it's very hard to change it or trick it. OCR (Optical Character Recognition) is like a smart scanner that can read and understand writing on papers or documents. It helps to make sure the information is correct. SECHash working: When a document comes in, it's scanned and the information is read by OCR the it checks if everything is right. If it's all good, the document's information is stored using the blockchain. Once it's stored, it can't be changed, lost, or destroyed. In its pursuit of higher accuracy in managing incoming invoices and bills, the project endeavours to transition from the current public LBRY to a private blockchain network. The goal is to fully automate the process by enhancing invoice data detection and extraction. Addressing the complexities of sharing government information, the initiative aims to overcome trust issues concerning data authenticity. This involves transitioning from an internet-based connection among departments to a more secure private network, ensuring decentralized data collection, storage, and processing. The fundamental objective remains to uphold data integrity and immutability.

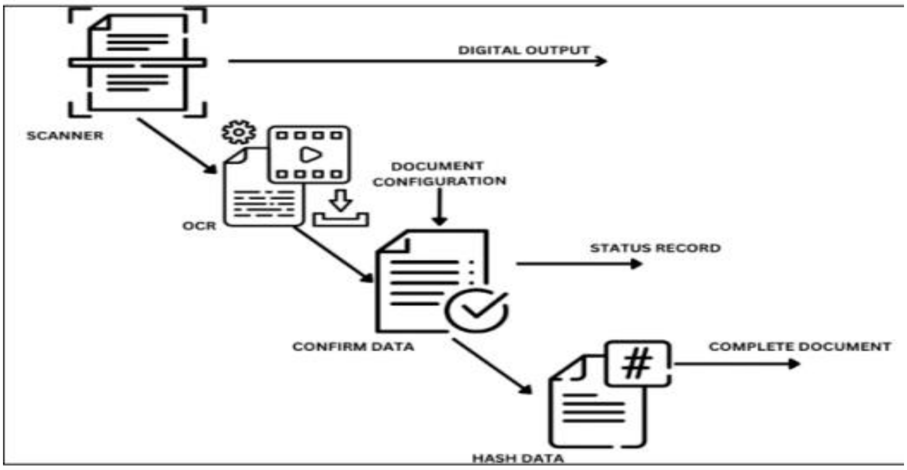

Fig:1 SECHash Model

The proposed system

In this system, users provide important details such as invoices or other private information using the userfriendly front-end interface. Data entry as source and Data is stored in a powerful and efficient database This storage located internally facilitates access to information needed for future work and business. Data stored using Optical Character Recognition (OCR) technology Complex processing is by identifying and extracting the content of data, images or a data type plays an important role in the system. More work. When text or data is extracted from the data, it moves to the key level and is cryptographically embedded in the Blockchain. The blockchain framework ensures the highest standards of security, immutability, and traceability for stored data. The data is processed and encrypted and becomes part of the blockchain, making it very secure and tamper-proof. Blockchain's unique features (distribution, distribution, cryptographic security, and immutability) provide a solid foundation for the security and integrity of the system.

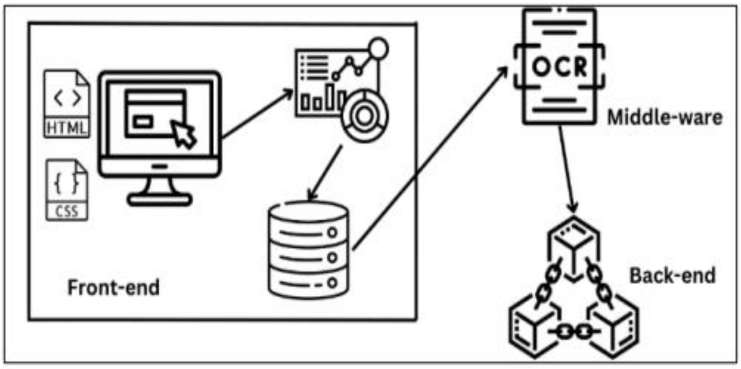

Fig : 2 Working Model

3. COMPONENTS OF THE MODEL

Front-end: The interface of our project comprises a simple login page, allowing users to log in using a username and the associated password. The technologies employed for this feature include HTML, CSS, and JavaScript. Upon entering the correct login details, the system securely stores this information in a database for future authentication and verification.

Middle-ware: OCR, or Optical Character Recognition is a type of technology that allows you to extract information from a document and turn it into searchable and editable data. Whether your documents are coming in as physical pieces of paper that need to be scanned in or something like a non-searchable PDF, OCR is going to allow you to digitize that information. And once we have extracted the information from a document, we are able to pass it along to other systems or a content management platform for process management down the line.

Back-end: Blockchain is a public record open to all. They make an interesting point: once some information is recorded on the blockchain, it is difficult to change it. Each block contains some information, including the hash of the block and the hash of the previous block. The data stored in a block depends on the type of blockchain. For example, the Bitcoin blockchain stores transaction details here, such as the sender, recipient, and number of coins. A block also has a hash value. You can compare the hash value with the fingerprint. It identifies the block and all its contents and is always unique, like a fingerprint. When a block is created, its hash is calculated. Changing anything in a block causes the hash to change. In other words, hashes are very useful when you want to capture changes to a block. If the block print changes, it is no longer the same. The third element of each block is the hash value of the previous block. This effectively creates a blockchain and is the technology that makes blockchains secure.

Key elements of blockchain:

• Distributed ledger technology: Each network shares a distributed ledger that records transactions. Using this shared data, transactions are recorded only once, eliminating the problems of traditional automated transaction processing.

• Immutable data: Once a transaction is recorded in a shared ledger, no participant can change or tamper with it. If there is an error in the list, a new change must be added to reverse the error so that both changes appear. In this way, we ensure that no one tries to change the private content.

• Smart Contracts: To speed up, transactions called smart contracts are stored on the blockchain and executed successfully. Smart contracts, travel insurance payment terms, etc. It can define the terms of change between companies, including Type: Public blockchains are decentralized peer-to-peer networks that anyone can join and participate in; for example, Bitcoin. However, they may require a lot of processing power, offer small transactions, and have poor security. On the other hand, private blockchains are peer-topeer collaborations managed by an organization. Organizations control who can participate, control the approval process, and control information sharing. Private blockchains differ from public blockchains such as Bitcoin and Ethereum in that access and permissions are restricted. In a private blockchain, access to the network is limited to those who agree to have greater control. These networks typically have fewer nodes verifying transactions, increasing speed. Use security measures to prioritize privacy and confidentiality, but the level of confidentiality may vary. There are special blockchains that provide control and efficiency for businesses. They are used in industries such as supply chain management, healthcare, and finance. Governance of private blockchains is generally more important than that of public blockchains; governance and operations are more important than full distribution.

Blockchain:

1. Web Applications vs Blockchain: In traditional web applications, rules and information are on a central server. Users access the application through a web browser and interact with the server. In contrast, blockchain-based applications store code and information through the blockchain network. User-defined forms in HTML, CSS, and JavaScript interact directly with the blockchain, eliminating the need for a central server.

2. Central vs. Decentralized: Traditional applications are centralized; This means managing rules and information in one place and allows for easy updates. In contrast, blockchain applications are decentralized because all data and code are distributed throughout the network of nodes. Changes to the blockchain require approval from network partners.

3. Code and statistics distribution: Users interact directly with the blockchain network to access code and data. It does not interact with the server but communicates with the blockchain to read, write, and execute transactions, all controlled by smart contracts.

4. Immutability and security: The decentralized structure of Blockchain ensures the immutability and security of information. Once data is recorded on the blockchain, it is difficult to change or manage it. Smart contracts are like private contracts with predefined rules that ensure transactions and operations are secure and transparent.

5. Peer-to-Peer Communication: Users interact with the blockchain network directly from their browser, making it easy to communicate with peers without any middle ground. The shift from centralized to decentralized blockchain applications has redefined the way we access, store data, and conduct business in terms of transparency, security, and flexibility in the process.

Advantage

1.Trust in government and Improved efficiency and accessibility: eGovGuard establishes trust in government operations through a transparent and secure data management system, assuring users of information accuracy and reliability. Utilizing Optical Character Recognition (OCR) tools to digitize physical archives, enhancing management efficiency and enabling easy access and modification of critical information. eGovGuard's use of private blockchain technology makes it versatile for sectors beyond government, such as supply chain management, healthcare, and finance, due to increased speed, control, and security.

2. Smart Contract Integration: Implementing smart contracts to streamline transactions, ensuring security, and accelerating document execution within a secure environment.

3. Digital protection: eGovGuard remains dedicated to ensuring the security and integrity of government information in the evolving digital landscape, benefiting citizens and government officials by maintaining reliable and secure information

4. CONCLUSION

The eGovGuard project is designed to enhance the security and integrity of government documents in the digital realm. It addresses issues faced by e-government initiatives, such as fraud and document tampering, by utilizing advanced technologies like blockchain, OCR, and smart contracts. Blockchain technology is the cornerstone of the project, ensuring data integrity and security. Using smart contracts written in Solidity, documents' details are securely stored on the blockchain, creating an immutable record that prevents tampering. The distinction between private and public blockchains is highlighted, with the project opting for a private blockchain to control access and permissions, particularly in sensitive government sectors like healthcare and finance. Overall, eGovGuard goes beyond being a technological solution—it acts as a safeguard for crucial government data, promoting transparency, data integrity, and trust within the government system in our increasingly digital world.

5. REFERENCES

[1] Fatima Azzam, Mariam Jaber, Amany Saies, Tareq Kirresh, Ruba Awadallah, Abdallah Karakra, Hafez Barghouthi, Saleh Amarneh. “The Use of Blockchain Technology and OCR in E-Government for Document Management: Inbound Invoice Management as an Example.” in Appl. Sci. 2023, 13(14), 8463.

[2] Salfrina Abdhullaha, Al Dulaimi Moatasem, Abdulmajeed Alwan, Yusmadi Yash Jusoh. “Blockchain Technologies in e-Government Services" in 2022 IEEE International Conference on Computing (ICOCO).

[3] Yiwei Zhang, Sanhong Deng∗ (corresponding author), Yue Zhang, Jia Kong. “Research on Government Information Sharing Model Using Blockchain Technology” in 2019 10th International Conference on Information Technology in Medicine and Education (ITME).

[4] Febriansyah, Darius Antoni, Endang Lestari "The Role of Blockchain Technology in E-Government Capability: Literature Review" in University of Exeter.

[5] Malodia, S.; Dhir, A.; Mishra, M.; Bhatti, Z.A. Future of e-Government: An integrated conceptual framework. Technol. Forecast. Soc. Chang. 2021, 173, 121102.

[6] Farida, I.; Setiawan, R.; Maryatmi, A.; Juwita, N. The Implementation of E-Government in the Industrial Revolution Era 4.0 in Indonesia. Int. J. Progress. Sci. Technol. 2020, 22, 340–346.

[7] Carter, L.; Yoon, V.; Liu, D. Analyzing e-government design science artifacts: A systematic literature review. Int. J. Inf. Manag. 2022, 62, 102430. Maulidi A. Philosophical understanding of the dynamics and control of occupational fraud in the public sector: Contingency analysis. Int. J. Ethics Syst. 2023, 39, 432–463.

[8] Tacconi, L.; Williams, D.A. Corruption, and anti-corruption in environmental and resource management. Annu. Rev. Environ. Resour. 2020, 45, 305–329.

[9] Dikmen, S.; Çiçek, H.G. Fighting Against Corruption and Bribery in Public Procurements during the COVID-19 Pandemic. The Ethics of Bribery: Theoretical and Empirical Studies; Springer: Cham, Switzerland, 2022; Volume 10.

[10] Awadallah, R.; Samsudin, A.; Teh, J.S.; Almazrooie, M. An Integrated Architecture for Maintaining Security in Cloud Computing Based on Blockchain. IEEE Access 2021, 9, 69513–69526.