Digital Certificate Fraud Detection Using Blockchain Technology

T P Arvindan[1,a)], M Balaji [2,b)], E V Divya Prasana[3,c)], K M Mohamed Salman[4,d)]

Author Affiliations

1,2,3,4Department of Computer Science and Engineering, Periyar Maniammai Institute of Science & Technology, Thanjavur, India

Author Emails

[a)] Arvindantp05@gmail.com
[b)] Balajimohan390@gmail.com
[c)] Divyaprasana30@gmail.com
[d)] Mohdsalman0300@gmail.com

ABSTRACT

Digital Certificate Fraud poses a significant threat to the integrity of various industries and institutions. In response to this challenge, a novel approach leveraging Blockchain Technology for the detection of certificate authenticity has been developed. This innovative system involves uploading digital certificates onto a blockchain, creating an immutable and decentralized ledger of certificates. Each certificate is uniquely identified, and its details are securely stored within the blockchain. Smart contracts are employed to automate the comparison process, ensuring that uploaded certificates are thoroughly examined for fraudulent elements. The decentralized nature of the blockchain enhances security, making it resistant to tampering and providing a transparent and traceable record of certificate transactions. This system not only streamlines the verification process but also significantly reduces the risk of certificate fraud by creating a reliable and auditable platform for certificate validation. Through the integration of Blockchain Technology, this solution offers a robust and efficient mechanism to combat digital certificate fraud, safeguarding the credibility of certificates and bolstering trust in various sectors.

INTRODUCTION

As our world becomes increasingly digitized, the reliance on digital certificates has grown exponentially, underpinning the security and authenticity of transactions, communications, and credentials across various industries. However, the escalating threat of digital certificate fraud poses a formidable challenge, compromising the very foundation of trust that these certificates are designed to establish. In response to this pressing issue, a ground breaking solution harnessing the power of Blockchain Technology has emerged. This innovative approach aims to revolutionize the detection and prevention of digital certificate fraud by leveraging the inherent security features of blockchain. The following exploration delves into the application of blockchain in the context of digital certificate fraud detection, offering a robust and decentralized framework to ensure the integrity of certificates in an increasingly interconnected and digital landscape.

BLOCK CHAIN

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Block chains are best known for their crucial role in crypto currency systems, such as Bitcoin, for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.

Blockchain, a revolutionary technology that emerged alongside the advent of cryptocurrencies, has evolved into a transformative force with implications reaching far beyond the financial sector. At its core, a blockchain is a decentralized and distributed ledger that records transactions across a network of computers in a secure, transparent, and tamper-resistant manner. Unlike traditional centralized systems, blockchain operates on a consensus mechanism, where each participant in the network has a copy of the entire ledger. This decentralized structure eliminates the need for a central authority, fostering trust and transparency among participants. Each block in the chain contains a set of transactions, and these blocks are linked together using cryptographic hashes. Once a block is added to the chain, it becomes virtually immutable, as altering the information in one block would require changing every subsequent block, a feat that is computationally infeasible and easily detectable. Blockchain technology brings forth several key features, including transparency, security, and decentralization. Smart contracts, self-executing contracts with the terms of the agreement directly written into code, further enhance the functionality of blockchain by automating and enforcing contractual agreements. Beyond its origins in cryptocurrency, blockchain is finding applications in various industries, such as supply chain management, healthcare, finance, and more. Its potential to revolutionize how we transact, share data, and establish trust in the digital age positions blockchain as a cornerstone technology for future innovations and disruptions.

How Does a Blockchain Work?

The goal of blockchain is to allow digital information to be recorded and distributed, but not edited. In this way, a blockchain is the foundation for immutable ledgers, or records of transactions that cannot be altered, deleted, or destroyed. This is why block chains are also known as a distributed ledger technology (DLT).

Blockchain Decentralization

Imagine that a company owns a server farm with 10,000 computers used to maintain a database holding all of its client's account information. This company owns a warehouse building that contains all of these computers under one roof and has full control of each of these computers and all of the information contained within them. This, however, provides a single point of failure. What happens if the electricity at that location goes out? What if its Internet connection is severed? What if it burns to the ground? What if a bad actor erases everything with a single keystroke? In any case, the data is lost or corrupted.

What a blockchain does is to allow the data held in that database to be spread out among several network nodes at various locations. This not only creates redundancy but also maintains the fidelity of the data stored therein—if somebody tries to alter a record at one instance of the database, the other nodes would not be altered and thus would prevent a bad actor from doing so. If one user tampers with Bit coin's record of transactions, all other nodes would cross-reference each other and easily pinpoint the node with the incorrect information. This system helps to establish an exact and transparent order of events. This way, no single node within the network can alter information held within it.

Is Blockchain Secure?

Blockchain technology achieves decentralized security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. After a block has been added to the end of the blockchain, it is extremely difficult to go back and alter the contents of the block unless a majority of the network has reached a consensus to do so. That's because each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned time stamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes as well.

What Is Blockchain Technology?

Blockchain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain," in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a 'digital ledger.'

Every transaction in this ledger is authorized by the digital signature of the owner, which authenticates the transaction and safeguards it from tampering. Hence, the information the digital ledger contains is highly secure.

In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which, the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can't corrupt it.

How Does Blockchain Technology Work?

In recent years, you may have noticed many businesses around the world integrating Blockchain technology. But how exactly does Blockchain technology work? Is this a significant change or a simple addition? The advancements of Blockchain are still young and have the potential to be revolutionary in the future; so, let's begin demystifying this technology.

Blockchain is a combination of three leading technologies:

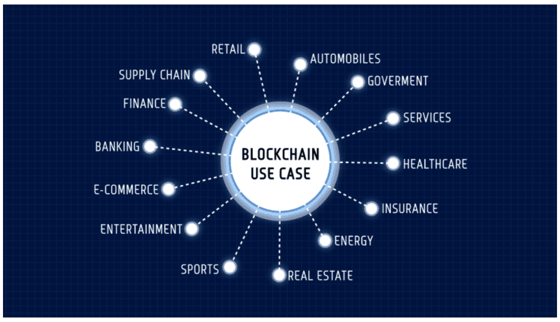
1. Cryptographic keys.

2. A peer-to-peer network containing a shared ledger.

3. A means of computing, to store the transactions and records of the network.

Cryptography keys consist of two keys – Private Key and Public key. These keys help in performing successful transactions between two parties. Each individual has these two keys, which they use to produce a secure digital identity reference. This secured identity is the most important aspect of Blockchain technology. In the world of crypto currency, this identity is referred to as 'digital signature' and is used for authorizing and controlling transactions.

APPLICATION



Cryptocurrencies:

The most well-known application of blockchain is in the creation and management of cryptocurrencies like Bitcoin and Ethereum. Blockchain ensures secure and transparent transactions without the need for a central authority.

Smart Contracts:

Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They automatically execute and enforce contract clauses when predefined conditions are met, providing transparency and reducing the need for intermediaries.

Supply Chain Management:

Blockchain enhances transparency and traceability in supply chains. Each transaction or movement of goods is recorded on the blockchain, enabling stakeholders to track the provenance of products, reduce fraud, and ensure the authenticity of goods.

Identity Management:

Blockchain can be used for secure and decentralized identity management. Individuals can control access to their personal information, reducing the risk of identity theft, and streamlining processes like KYC (Know Your Customer) verification.

Healthcare Records:

Blockchain secures the storage and sharing of healthcare records. Patients have control over their data, and healthcare providers can access a complete and accurate medical history, improving the quality of care and reducing errors.

Voting Systems:

Blockchain can be applied to create transparent and tamper-resistant voting systems. Each vote is recorded on the blockchain, ensuring the integrity of the election process and reducing the risk of fraud.

Cross-Border Payments:

Blockchain facilitates faster and more cost-effective cross-border payments by eliminating intermediaries and providing a transparent and secure ledger for tracking transactions.

Real Estate:

Blockchain simplifies real estate transactions by reducing the need for paperwork and intermediaries. Smart contracts can automate tasks like property transfers and payments, streamlining the buying and selling process.

Intellectual Property Protection:

Blockchain can be used to timestamp and authenticate intellectual property, such as patents, copyrights, and trademarks. This ensures a transparent record of ownership and helps in preventing infringement.

Energy Trading:

In the energy sector, blockchain enables peer-to-peer energy trading. Producers can sell excess energy directly to consumers in a transparent and decentralized manner, fostering a more efficient and sustainable energy ecosystem.

OBJECTIVE

- Digital certificate fraud detection using blockchain technology is an approach to enhance the security and integrity of digital certificates.
- A digital certificate that employs digital signature technology, authorizations to validate the user's identity in digital fields, and the authority to utilize network resources.
- This allows companies to check employees' educational documents during the recruitment process and saves time testing the educational documents.

LITERATURE SURVEY

2.1 TITLE: A New Decentralized Certification Verification Privacy Control Protocol

AUTHOR: Omar S. Saleh, Osman Ghazali, Norbik Bashah Idris

YEAR:2021

DESCRIPTION: Academic Certificates are a social convention that offers a forum for new knowledge about a person or an entity to be transmitted. Academic certificates are one of the areas of education in which the short-term application of blockchain technology can be seen. The practice of certificate fraud is common, undermining investment and trust in higher education systems and bearing substantial economic and social. Falsified qualifications vary from diplomas in high school to doctoral degrees. In addition, the credentials of several famous universities have been forged and it is very difficult to detect such forgeries. Hence, blockchain was introduced to improve the verification process of academic certificates. Recently, blockchain technology has emerged as a potential way of authenticating the process of document authentication and as an effective tool for combating document fraud and misuse. Blockchain based applications have been developed by various Universities. However, privacy preserving was a challenge in most of the existing solutions. Privacy indicates that the certificate protects both identity and information. Therefore , a new Decentralized Certification Verification Privacy Control Protocol is proposed. The proposed protocol can be used for issuing and verifying educational certificates while maintaining privacy and confidentiality at the network level (Ministries level, Universities level, Students level) and data level. The decentralized solution was implemented using Hyperledger Fabric as the infrastructure and Javascript as the contract language.

2.2 TITLE: The benefits of blockchain for digital certificates: A multiple case study analysis

AUTHOR: Shuyi Pu, Jasmine Siu Lee Lam

YEAR: 2023

DESCRIPTION: Certificates in either hard or soft copies are common documents in our day-to-day activities. However, they are vulnerable to be tampered and inefficiencies exist in the current verification systems. Blockchain technology is considered a feasible solution to protect certificates from being forged and simplify the current verification systems. As an attempt to understand the potential of blockchain for digital certificates in a holistic view, this research aims to conduct a deep analysis of the benefits of blockchain for digital certificates using a multiple case study approach. A benefits analysis model is developed for mapping the benefits of an information system comprehensively and systematically covering benefits in technical, individual, organisational and societal dimensions. Although contextual variations exist, some common benefits are identified such as reduced costs of verification, improved decision making and planning, attracting new customers and supporting business growth. Lastly, future research opportunities in this research field are identified.

2.3 TITLE: A Review of Cyber Security and Blockchain

AUTHOR: Silvana Qose; Beatrix Fregan

YEAR:2022

DESCRIPTION: Since the introduction of the Blockchain in Satoshi Nakamoto's study in 2008, Blockchain has become one of the foremost often mentioned ways to secure information storage and transfers for the trustless. This article is based on a literature review of decentralized technology and peer-to-peer systems that represents a scientific analysis of the most frequently adopted blockchain security applications in the usage of the Blockchain for cyber security functions. The findings indicate that the Internet of Things (IoT) and networks, machine visualization, and public-key cryptography hands themselves innovative to blockchain applications, just like safe storage of Personally Identifiable Information or online applications and certification schemes. This is a well-timed study based on systematic studies from several scientific journals. It will be an additional mild assessment of future prospects in Blockchain and cyber security research and blockchain security for AI data, including the safety of Blockchain in IoT and sidechain safety.

2.4 TITLE: Bank Fraud Detection using Community Detection Algorithm

AUTHOR: Dhiman Sarma, Wahidul Alam

YEAR:2020

DESCRIPTION: Bank fraud is a federal crime that involves fraudulent attempts aims for monetary gains by deceiving financial institutions. Every year, banks and financial institutions lose billions due to fraud. Fraudsters tempt bankers through scams to gain financial assets. The most common types of bank fraud include debit and credit card fraud, account fraud, insurance fraud, money laundering fraud, etc. Bankers are obliged to safeguard their financial assets as well as institutional integrity to armored the global financial system. Anti-fraud guard systems are regularly circumvented by fraudsters' dodging techniques. This paper proposed a system to detect bank fraud using a community detection algorithm that identifies the patterns that can lead to fraud occurrences. An agile method was used to design the web-based application to detect the fraud. The application functioned as a central hub between the banks and customers. Neo4j, a graph database, was used for creating and representing the database, and the Cypher query was used as a graph query language. The proposed system successfully detected all frauds presented during the test experiment. This paper will assist bankers to combat fraud by detecting and preventing similar occurrences.

2.5 TITLE: Credit Card Fraud Detection Using Machine Learning Techniques

AUTHOR: Indrani Vejalla, Sai Preethi Battula, Kartheek Kalluri

YEAR: 2023

DESCRIPTION: There are many types of fraud in our daily life. One of the frauds occurring these days is credit card fraud. When people around the globe make credit card transactions, there will also be fraudulent transactions. To avoid credit card fraud, we must know the patterns and how the fraud values differ. This paper proposed credit card fraud detection using machine learning based on the labeled data and differentiating the fraudulent and legitimate transactions. The experiment was conducted using supervised machine-learning techniques. Fraud is deceiving someone into intentionally giving up on their properties, money, or any legal rights, resulting in financial or personal gain for the illegitimate person. Many fraud types occur in our daily lives, including credit card fraud. Fraud in credit card transactions can be given to an illegitimate person using the card details and making beneficial transactions. Credit card fraud will result in a loss of money for the legitimate cardholder. Credit card fraud is one of the leading problems in the world. In 2020 the fraud in credit card cases had increased to 45,120. The rise in both online transactions has led to more fraud in credit cards. Prevention measures can be taken to stop this fraud by studying the behavior and patterns associated with fraudulent transactions

2.6 TITLE: Deep CNN approach for Unbalanced Credit Card Fraud Detection Data

AUTHOR: Mohammad Ziad Mizher, Ali Bou Nassif

YEAR: 2023

DESCRIPTION: Recent developments in electronic payment technologies have significantly increased the volume of daily online transactions and payments via credit cards. As internet use grows exponentially, it naturally follows that there is also a rise in credit card fraud, which is having a big effect on many organizations, including those in the financial industry. To detect risks such as fraudulent transactions and nonuniform attacks, the development of advanced financial detection mechanisms proactively completes the required task. However, these problems have been addressed by machine learning techniques on a large scale over the past years. Hence, these techniques need some improvement in terms of identifying unfamiliar attack patterns, velocity calculations, and big data analysis. In this paper, we propose a convolutional neural network approach (CNN) along with two machine learning algorithms to tackle the issue of credit card fraud detection. Our proposed models were evaluated and compared when dealing with large amounts of data using a highly imbalanced real-world credit card fraud detection dataset. Python programming languages were used to preprocess the data and test the model's measurements and performance. As observed in the results, an accuracy of 99.7% using the Random Forest classifier was obtained, which achieved a superior result in comparison to other models.

2.7 TITLE: Education Degree Fraud Detection and Student Certificate Verification using Blockchain

AUTHOR: Jayesh G. Dongre, Dr.Kishore.T.Patil

YEAR:2020

DESCRIPTION: To verify the authenticity of an academic degree and certificates we propose a system which employs a digital signature scheme and timestamps using blockchain technology. As the number of universities and tertiary education students, the number of graduates is constantly increasing. Due to this verification process of these degree certificates generates a lot of new job opportunities. The sudden changes in the technology and development of new technologies like blockchain is booming, the implementation of blockchain using blockcerts software provides us a solution of plausible business models. In this paper we showcase two financial models balancing where the service rates is been balanced between graduates and employer as to main stakeholders of that service. A proof check of certificates for students is done at low cost and an easy check of the authenticity of the certificate is done from and trustable source while recruiting by the employer. Proving unambiguously that you have an academic certificate (university degree, doctorate, or any certification of studies) is a process that changes in each country or institution of education. Some academic centres allow a quick and simple online query to verify the authenticity of their certificates, without even asking who requires that information. Some assign the role to third parties (whether by default or as required by regulations) or market the service. Finally, there are times when there is no alternative but to contact the office of the academic secretary at the educational institution directly, so that we can confirm if a diploma or qualification is valid or not. While, academic credential fraud is a fact and comes through counterfeiting, as well as through the involvement of the authorities and employees of the institution. The frequency of these events is also adequate to detect the emergence of dedicated companies

2.8 TITLE: Online Transaction Fraud Detection System Based on Machine Learning

AUTHOR: Virjanand, Rajkishan Bharti, Shubham Chauhan

YEAR: 2022

DESCRIPTION: Transaction fraud is a major cause of concern. As online transactions become more popular, so do the types of online transaction fraud that accompany them, affecting the financial industry. This fraud detection system is capable of restricting and impeding an attacker's transaction using credit card information of a genuine user. By allowing transactions that exceed the customer's current transaction limit, this system was designed to address these issues. In order to detect fraudulent user behavior, we gather the necessary information at registration. The details of items purchased by any individual transaction are generally unknown to any Fraud Detection System (FDS) running at the bank that issues credit cards to cardholders. BLA is being used to resolve this problem (Behavior and Location Analysis). A FDS is a credit card issuing bank. Every pending transaction is sent to the FDS for approval. To determine whether or not the transaction is genuine, FDS receives the card information and transaction value. The FDS has no understanding of the technology purchased in that transaction. The bank refuses the transaction if FDS confirms it is fraudulent. If an unexpected pattern is identified, the system must be re-verified using the users' spending habits and geographic location. The system detects unusual patterns in the payment procedure based on the user's previous information. After three unsuccessful attempts, the system will ban the user. The new electronic transaction era needs the detecting of fraud in online transactions. It's extremely difficult to improve the consistency and stability of the fraud detection model because customer transaction patterns and offenders' fraud behavior are constantly changing. In this report, we'll examine about how a deep neural network's loss function affects the acquisition of deep feature representations of legitimate and fraudulent transactions.

2.9 TITLE: Credit Card Fraud Detection Using Machine Learning Techniques

AUTHOR: Indrani Vejalla, Sai Preethi Battula

YEAR:2023

DESCRIPTION: There are many types of fraud in our daily life. One of the frauds occurring these days is credit card fraud. When people around the globe make credit card transactions, there will also be fraudulent transactions. To avoid credit card fraud, we must know the patterns and how the fraud values differ. This paper proposed credit card fraud detection using machine learning based on the labeled data and differentiating the fraudulent and legitimate transactions. The experiment was conducted using supervised machine-learning techniques. Fraud is deceiving someone into intentionally giving up on their properties, money, or any legal rights, resulting in financial or personal gain for the illegitimate person. Many fraud types occur in our daily lives, including credit card fraud. Fraud in credit card transactions can be given to an illegitimate person using the card details and making beneficial transactions. Credit card fraud will result in a loss of money for the legitimate cardholder. Credit card fraud is one of the leading problems in the world. In 2020 the fraud in credit card cases had increased to 45,120. The rise in both online transactions has led to more fraud in credit cards. Prevention measures can be taken to stop this fraud by studying the behavior and patterns associated with fraudulent transactions. Due to the rise of online transactions, credit card usage is increasing. Most of the transactions are online, which requires credit/debit card transactions. Without knowing, credit cards play an essential role in our daily lives. When people around the globe make credit card transactions, there will also be fraudulent transactions, so machine learning techniques help to detect these types of fraud.

2.10 TITLE: Fraud Detection: A Review on Blockchain

AUTHOR: Anuska Rakshit, Shriya Kumar, Ramanathan L

YEAR: 2022

DESCRIPTION: A blockchain is a distributed database of records, commonly known as a public book, of all completed transactions or digital events that may be shared between participants. Most program participants double check each activity in the community manual. Once the data is entered, it will never be erased. Keeping track of what is being done permanently, implicitly, and irrevocably, can help prevent many types of information fraud. Fraudulent transactions cannot surpass accumulated guarantees and guarantees as each transaction must be made by a group of miners. With moderate data storage and administrative systems, hacking, hacking, and breach are all possible, but the widespread blockchain compliance mechanism prevents this. Any asset, goods, or service may be directed. Identity theft, fraud, and network or system failure. On the Internet, malicious behavior includes identity theft, fraud, and network or system intrusion. Blockchain-based trading has to deal with challenges such as online fraud, identity theft, and fraud. We will examine how blockchain technology works in detecting fraud in this study. While there are many more types of information fraud, we will focus on a few of the most common ones in this study, such as rating fraud, insurance fraud, employment history fraud, fraudulent acquisition fraud, and various other fraudulent scams. our industries.

EXISTING SYSTEM

In the existing system presents the development of an intelligent certificate verification system for fraud detection using machine learning technique. The research was embarked upon after noticing the rate of document forgery in the Nigerian society. Thus an exhaustive review of literatures was made which identified the challenges public and private institutions encounter due to lack of automated means to verify any legal document. The Methodology used for the development of the proposed system are image processing, artificial intelligence and object oriented analysis methodology. This research seeks to address the problems via the development of a machine learning based verification system and localizing it for the verification of certificate. Today, in both the public and private enterprises, the traditional means of document verification is via observation method where documents are observed and then automatically accepted for certain actions or proceedings based on signatures, stamps, seals, etc. However, these criteria used for authenticating documents are very easy to be reproduced and commit fraud, and as a result has become a major problem, as the daily media hardly make broadcast today all over the world without citing a scenario of fraud with fake documents. One of the document types which is the current trend today is the fabrication of fake certificates. Certificates are official documents given by an organization to certain qualified persons as a proof that the person has completed a certain professional training, course, study or program. This document is accepted worldwide for employment, education, training purposes etc.

DISADVANTAGE

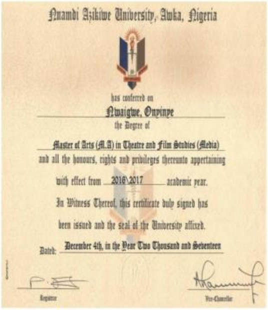
- Complex models can be difficult to interpret.
- If not carefully managed, models can overfit to the training data, which means they perform well on the training data but poorly on new, unseen data.
- This can result in lower fraud detection rates

PROPOSED SYSTEM

The proposed system for Digital Certificate Fraud Detection using Blockchain Technology is a cutting-edge solution designed to fortify the integrity of digital certificates. This innovative framework involves uploading digital certificates onto a blockchain, creating a decentralized and tamper-resistant ledger. The core functionality lies in the rigorous comparison process, where the uploaded certificates are systematically scrutinized to ascertain their authenticity. Leveraging the inherent characteristics of blockchain, each certificate is uniquely identified and securely stored, rendering any attempt at fraud or unauthorized alterations virtually impossible. The system utilizes smart contracts to automate the verification process, expediting the identification of fraudulent elements and streamlining the overall certificate validation. Through the transparent and traceable nature of the blockchain, authorized entities can efficiently verify the legitimacy of certificates in real-time. The decentralized architecture ensures that the credibility of certificates remains intact, significantly mitigating the risks associated with digital certificate fraud. By prioritizing security, efficiency, and transparency, the proposed system aims to establish a robust foundation for combating fraudulent activities and upholding the trustworthiness of digital certificates across diverse industries.

CERTIFICATE FRAUD DETECTION

The certificate fraud detection system operates through a meticulous and secure process leveraging blockchain technology. Initially, the digital certificates, such as academic degrees or professional qualifications, are uploaded onto the blockchain. Each certificate is uniquely identified and securely stored in a decentralized ledger, utilizing the tamper-resistant properties of blockchain. The system employs smart contracts to automate the verification process. These contracts execute predefined rules and conditions to compare the details within the uploaded certificates, ensuring their authenticity. During this comparison, the system checks for any irregularities, unauthorized alterations, or potential signs of fraud. If the certificate passes this verification stage, it is considered authentic and is recorded on the blockchain. This decentralized and transparent ledger provides a real-time and immutable record of verified certificates. Authorized parties, such as employers or educational institutions, can then independently and efficiently validate the authenticity of a certificate by querying the blockchain. Any attempt at fraud or tampering is mitigated by the decentralized and trustless nature of blockchain technology. Additionally, the system prioritizes user data privacy through cryptographic techniques, ensuring that only authorized parties have access to sensitive information. In summary, the working process of the certificate fraud detection system involves secure uploading, automated verification through smart contracts, and decentralized validation via blockchain, collectively establishing a robust mechanism to combat digital certificate fraud.



Nnamdi Azikiwe University, Awka, Nigeria

has conferred on

Nwaigwe, Onyinye

the Degree of

Master of Arts (M.A) in Theatre and Film Studies (Media)

and all the honours, rights and privileges thereunto appertaining

with effect from 2016\2017 academic year.

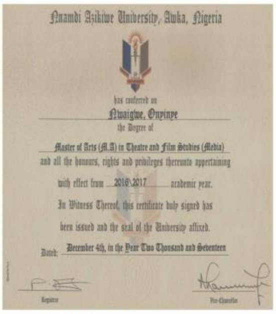
In Witness Thereof, this certificate duly signed has

been issued and the seal of the University affixed.

Dated: December 4th, in the Year Two Thousand and Seventeen

Registrar

Vice-Chancellor



Nnamdi Azikiwe University, Awka, Nigeria

has conferred on

Nwaigwe, Onyinye

the Degree of

Master of Arts (M.A) in Theatre and Film Studies (Media)

and all the honours, rights and privileges thereunto appertaining

with effect from 2016\2017 academic year.

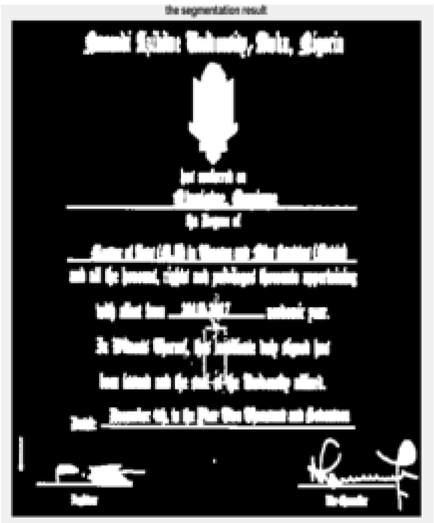
In Witness Thereof, this certificate duly signed has

been issued and the seal of the University affixed.

Dated: December 4th, in the Year Two Thousand and Seventeen

Registrar

Vice-Chancellor



Forgery Prevention:

One of the primary concerns is preventing the forgery of physical or digital certificates. This involves implementing security features, such as holograms, watermarks, or digital signatures that are difficult to replicate. For digital certificates, encryption and secure key management are crucial to prevent unauthorized alterations.

Verification Mechanisms:

Establishing robust verification mechanisms is essential. This includes developing secure methods for entities, such as employers or educational institutions, to verify the authenticity of certificates. Traditional methods may involve contacting issuing institutions directly, but more advanced systems use technology, such as blockchain, to streamline and automate this process securely.

Blockchain Technology:

Blockchain technology has emerged as a powerful tool in certificate fraud detection. Certificates stored on a blockchain are tamper-resistant and transparent. Each certificate is assigned a unique identifier and recorded in a decentralized ledger, making it virtually impossible to alter or counterfeit.

Blockchain facilitates real-time verification by authorized parties, ensuring the credibility of certificates.

Data Privacy and Security:

Protecting the privacy and security of certificate holder data is crucial. Robust encryption methods and secure storage practices must be implemented to prevent unauthorized access to sensitive information. Compliance with data protection regulations is imperative to maintain the trust of certificate holders.

Machine Learning and AI:

Utilizing machine learning and artificial intelligence can enhance fraud detection capabilities. These technologies can analyze patterns, identify anomalies, and detect irregularities in certificate data or verification processes, providing an additional layer of security.

Multi-Factor Authentication (MFA):

Implementing multi-factor authentication adds an extra layer of security to the certificate verification process. By requiring multiple forms of identification, such as passwords, biometrics, or one-time codes, the system becomes more resilient to unauthorized access.

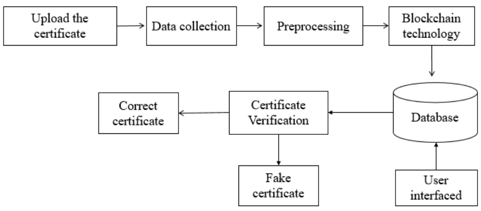
Regular Audits and Monitoring:

Regularly auditing and monitoring the certificate issuance and verification processes is essential. This involves conducting periodic reviews, analysing access logs, and staying vigilant for any unusual patterns or activities that may indicate fraudulent behaviour.

Education and Awareness:

Educating both certificate issuers and verifiers about the risks and signs of certificate fraud is crucial. Awareness programs can help institutions and organizations stay informed about evolving threats and implement proactive measures to prevent fraud.

BLOCK DIAGRAM



ADVANTAGE

- In the blockchain technology for digital certificate fraud detection can lead to cost savings in the long run. It reduces the need for centralized intermediaries and manual verification processes. This not only saves time but also reduces operational costs and the risk of human error in certificate verification.
- Digital certificates stored on a blockchain benefit from the robust security features inherent to blockchain technology. The decentralized and cryptographic nature of blockchains significantly reduces the risk of data breaches and unauthorized access. This ensures that only authorized parties can access and verify digital certificates

MODULE LIST

- Certificate Issuance Module
- Blockchain Integration Module
- Identity Verification Module
- Certificate Validation Module
- Fraud Detection and Monitoring Module

MODULE DESCRIPTION

Certificate Issuance Module:

- This module manages the issuance of digital certificates to individuals or entities.
- It includes functionalities for inputting and verifying the information to be included in the certificate.
- Ensures that only valid and authorized certificates are entered into the system.

Blockchain Integration Module:

- Establishes a connection with the blockchain network for storing and retrieving certificate data.
- Implements protocols for secure and decentralized storage of digital certificates on the blockchain.
- Manages the interaction between the system and the blockchain, ensuring seamless integration.

Identity Verification Module:

- Incorporates identity verification mechanisms to confirm the authenticity of the individuals or entities receiving the digital certificates.
- Utilizes multi-factor authentication or other secure methods to enhance the accuracy of identity verification.

Certificate Validation Module:

- Provides tools and processes for validating digital certificates in real-time.
- Allows users to independently verify the authenticity of a certificate by querying the blockchain.
- Ensures that the certificate information matches the details stored on the blockchain**.**

Fraud Detection and Monitoring Module:

- Implements algorithms and rules for detecting potential fraud or tampering with digital certificates.
- Monitors the blockchain for any suspicious activities or deviations from expected patterns.
- Generates alerts or notifications for administrators or users when potential fraud is detected.

SYSTEM REQUIREMENTS

H/W SYSTEM CONFIGURATION:-

- processor - Pentium – IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB

S/W SYSTEM CONFIGURATION:-

- Operating System : Windows 7 or 8
- Software : python Idle

PYTHON INTRODUCTION

Python is a high-level, versatile programming language that has gained immense popularity among developers and businesses due to its simplicity, readability, and extensive standard library. It was created by Guido van Rossum and first released in 1991, and since then, it has become one of the most widely used programming languages for a wide range of applications. Python's design philosophy emphasizes code readability and maintainability, making it an excellent choice for beginners and experienced developers alike. Python is an interpreted language, meaning it does not require compilation before execution, making it easy to write, test, and debug code. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming, giving developers the flexibility to approach problems from various angles. Python's extensive standard library provides a wealth of modules and packages that facilitate a wide range of tasks, from web development and data analysis to artificial intelligence and scientific computing. Python's simplicity and readability have made it a preferred choice for many domains, from web development using frameworks like Django and Flask to data analysis and machine learning with libraries such as NumPy, Pandas, and TensorFlow. Its versatility, combined with a vibrant and active community of developers, has solidified Python's position as a top programming language, making it an excellent tool for creating software solutions across diverse industries and applications. Whether you're a beginner learning to program or an experienced developer seeking a powerful and efficient language, Python offers a rich ecosystem and a supportive community to help you succeed in your software development endeavors.

Python IDLE

Python default IDE is known as IDLE (Integrated Development and Learning Environment). There is no need to install this IDE separately (via Python PIP) as it comes as default with Python installation. Although there are plenty of IDE which you can download separately on your system, still it is considered as a super choice for a newbie. IDLE comes by default on Windows and Mac but Linux user has to download it using the package manager. You have learned to write a Python code in Interactive environment, where you get the instant result of an expression. Now it's time to write a few lines of code to solve a problem. You can write multiple lines of code in the Interactive environment as well, but it is not favoured because of the debugging reasons.

FEATURES OF PYTHON

Easy to Learn and Use

Python is easy to learn and use compared with other programming languages. It is developer-friendly and high level programming language.]

Interpreted Language

Python is an interpreted language because no need of compilation. This makes debugging easy and thus suitable for beginners.

Cross-platform Language

Python can run equally on different platforms such as Windows, Linux, Unix and Macintosh etc. So, we can say that Python is a portable language.

Free and Open Source

The Python interpreter is developed under an open-source license, making it free to install, use, and distribute.

Object-Oriented Language

Python supports object oriented language and concepts of classes and objects come into existence.

GUI Programming Support

Graphical user interfaces can be developed using Python.

Integrated

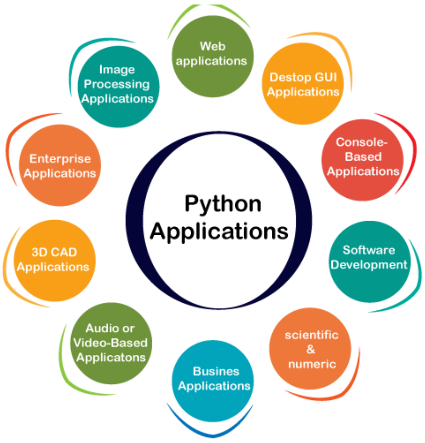
It can be easily integrated with languages like C, C++, and JAVA etc.

ADVANTAGE

- Python IDLE is an interactive shell that enables users to easily test and run short bits of Python code without needing to create a whole programme.
- Python IDLE's code editor has features like syntax highlighting and code completion that make it simpler and faster to write Python programmes.
- Python IDLE has a built-in debugger that enables programmers to walk through their code and find faults and problems.
- Python IDLE may be used on Linux, macOS, and Windows thanks to its cross-platform nature.
- Python IDLE is included with the Python installation, thus users don't need to install any more programmes in order to begin coding in Python.
- Python IDLE is open-source, free software, which entitles users to use it with no any limitations for both business and non-commercial uses.

APPLICATIONS

Python is known for its general-purpose nature that makes it applicable in almost every domain of software development. Python makes its presence in every emerging field. It is the fastest-growing programming language and can develop any application.



Web Applications

We can use Python to develop web applications. It provides libraries to handle internet protocols such as HTML and XML, JSON, Email processing, request, beautifulSoup, Feedparser, etc. One of Python web-framework named Django is used on Instagram. Python provides many useful frameworks, and these are given below:

- Django and Pyramid framework(Use for heavy applications)
- Flask and Bottle (Micro-framework)
- Plone and Django CMS (Advance Content management)

Desktop GUI Applications

The GUI stands for the Graphical User Interface, which provides a smooth interaction to any application. Python provides a Tk GUI library to develop a user interface. Some popular GUI libraries are given below.

- Tkinter or Tk
- wxWidgetM
- Kivy (used for writing multitouch applications)
- PyQt or Pyside

Console-based Application

Console-based applications run from the command-line or shell. These applications are computer program which are used commands to execute. This kind of application was more popular in the old generation of computers. Python can develop this kind of application very effectively. It is famous for having REPL, which means the Read-Eval-Print Loop that makes it the most suitable language for the command-line applications.

Python provides many free library or module which helps to build the command-line apps. The necessary IO libraries are used to read and write. It helps to parse argument and create console help text out-of-the-box. There are also advance libraries that can develop independent console apps.

Software Development

Python is useful for the software development process. It works as a support language and can be used to build control and management, testing, etc.

- SCons is used to build control.
- Buildbot and Apache Gumps are used for automated continuous compilation and testing.
- Round or Trac for bug tracking and project management.

Scientific and Numeric

This is the era of Artificial intelligence where the machine can perform the task the same as the human. Python language is the most suitable language for Artificial intelligence or machine learning. It consists of many scientific and mathematical libraries, which makes easy to solve complex calculations.

Implementing machine learning algorithms require complex mathematical calculation. Python has many libraries for scientific and numeric such as Numpy, Pandas, Scipy, Scikit-learn, etc. If you have some basic knowledge of Python, you need to import libraries on the top of the code. Few popular frameworks of machine libraries are given below.

- SciPy
- Scikit-learn
- NumPy
- Pandas
- Matplotlib

Business Applications

Business Applications differ from standard applications. E-commerce and ERP are an example of a business application. This kind of application requires extensively, scalability and readability, and Python provides all these features.

Oddo is an example of the all-in-one Python-based application which offers a range of business applications. Python provides a Tryton platform which is used to develop the business application.

Audio or Video-based Applications

Python is flexible to perform multiple tasks and can be used to create multimedia applications. Some multimedia applications which are made by using Python are TimPlayer, cplay, etc. The few multimedia libraries are given below.

- Gstreamer
- Pyglet

- QT Phonon

3D CAD Applications

The CAD (Computer-aided design) is used to design engineering related architecture. It is used to develop the 3D representation of a part of a system. Python can create a 3D CAD application by using the following functionalities.

- Fandango (Popular)
- CAMVOX
- HeeksCNC
- AnyCAD
- RCAM

Enterprise Applications

Python can be used to create applications that can be used within an Enterprise or an Organization. Some real-time applications are OpenERP, Tryton, Picalo, etc.

Image Processing Application

Python contains many libraries that are used to work with the image. The image can be manipulated according to our requirements. Some libraries of image processing are given below.

- OpenCV
- Pillow
- SimpleITK

PYTHON ABSTRACT SYNTAX

The compiler.ast module defines an abstract syntax for Python. In the abstract syntax tree, each node represents a syntactic construct. The root of the tree is Module object.

The abstract syntax offers a higher level interface to parsed Python source code. The parser module and the compiler written in C for the Python interpreter use a concrete syntax tree. The concrete syntax is tied closely to the grammar description used for the Python parser. Instead of a single node for a construct, there are often several levels of nested nodes that are introduced by Python's precedence rules.

The abstract syntax tree is created by the compiler.transformer module. The transformer relies on the built-in Python parser to generate a concrete syntax tree. It generates an abstract syntax tree from the concrete tree.

The transformer module was created by Greg Stein and Bill Tutt for an experimental Python-to-C compiler. The current version contains a number of modifications and improvements, but the basic form of the abstract syntax and of the transformer are due to Stein and Tutt.

AST NODES

The compiler.ast module is generated from a text file that describes each node type and its elements. Each node type is represented as a class that inherits from the abstract base class compiler.ast.Node and defines a set of named attributes for child nodes.

class compiler.ast.Node

The Node instances are created automatically by the parser generator. The recommended interface for specific Node instances is to use the public attributes to access child nodes. A public attribute may be bound to a single node or to a sequence of nodes, depending on the Node type. For example, the bases attribute of the Class node, is bound to a list of base class nodes, and the doc attribute is bound to a single node.

Each Node instance has a lineno attribute which may be None. XXX Not sure what the rules are for which nodes will have a useful lineno.

All Node objects offer the following methods:

getChildren()

Returns a flattened list of the child nodes and objects in the order they occur. Specifically, the order of the nodes is the order in which they appear in the Python grammar. Not all of the children are Node instances. The names of functions and classes, for example, are plain strings.

getChildNodes()

Returns a flattened list of the child nodes in the order they occur. This method is like getChildren(), except that it only returns those children that are Node instances.

The While node has three attributes: test, body, and else_. (If the natural name for an attribute is also a Python reserved word, it can't be used as an attribute name. An underscore is appended to the word to make it a legal identifier, hence else_ instead of else.)

The if statement is more complicated because it can include several tests.

The If node only defines two attributes: tests and else_. The tests attribute is a sequence of test expression, consequent body pairs. There is one pair for each if/elif clause. The first element of the pair is the test expression. The second elements is a Stmt node that contains the code to execute if the test is true.

The getChildren() method of If returns a flat list of child nodes. If there are three if/elif clauses and no else clause, then getChildren() will return a list of six elements: the first test expression, the first Stmt, the second text expression, etc.

The following table lists each of the Node subclasses defined in compiler.ast and each of the public attributes available on their instances. The values of most of the attributes are themselves Node instances or sequences of instances. When the value is something other than an instance, the type is noted in the comment. The attributes are listed in the order in which they are returned by getChildren() and getChildNodes().

DEVELOPMENT ENVIRONMENTS:

Most Python implementations (including CPython) include a read–eval–print loop (REPL), permitting them to function as a command line interpreter for which the user enters statements sequentially and receives results immediately.

Other shells, including IDLE and IPython, add further abilities such as auto-completion, session state retention and syntax highlighting.

IMPLEMENTATIONS

Reference implementation

CPython is the reference implementation of Python. It is written in C, meeting the C89 standard with several select C99 features. It compiles Python programs into an intermediate bytecode which is then executed by its virtual machine. CPython is distributed with a large standard library written in a mixture of C and native Python. It is available for many platforms, including Windows and most modern Unix-like systems. Platform portability was one of its earliest priorities.

Other implementations

PyPy is a fast, compliant interpreter of Python 2.7 and 3.5. Its just-in-time compiler brings a significant speed improvement over CPython but several libraries written in C cannot be used with it.

Stackless Python is a significant fork of CPython that implements microthreads; it does not use the C memory stack, thus allowing massively concurrent programs. PyPy also has a stackless version.

MicroPython and CircuitPython are Python 3 variants optimized for microcontrollers. This includes Lego Mindstorms EV3.

RustPython is a Python 3 interpreter written in Rust.

Unsupported implementations

Other just-in-time Python compilers have been developed, but are now unsupported:

Google began a project named Unladen Swallow in 2009, with the aim of speeding up the Python interpreter five-fold by using the LLVM, and of improving its multithreading ability to scale to thousands of cores, while ordinary implementations suffer from the global interpreter lock.

Psyco is a just-in-time specialising compiler that integrates with CPython and transforms bytecode to machine code at runtime. The emitted code is specialized for certain data types and is faster than standard Python code.

In 2005, Nokia released a Python interpreter for the Series 60 mobile phones named PyS60. It includes many of the modules from the CPython implementations and some additional modules to integrate with the Symbian operating system. The project has been kept up-to-date to run on all variants of the S60 platform, and several third-party modules are available. The Nokia N900 also supports Python with GTK widget libraries, enabling programs to be written and run on the target device.

Cross-compilers to other languages

There are several compilers to high-level object languages, with either unrestricted Python, a restricted subset of Python, or a language similar to Python as the source language:

- Jython enables the use of the Java class library from a Python program.
- IronPython follows a similar approach in order to run Python programs on the .NET Common Language Runtime.
- The RPython language can be compiled to C, and is used to build the PyPy interpreter of Python.
- Pyjs compiles Python to JavaScript.
- Cython compiles Python to C and C++.
- Numba uses LLVM to compile Python to machine code.
- Pythran compiles Python to C++.
- Somewhat dated Pyrex (latest release in 2010) and Shed Skin (latest release in 2013) compile to C and C++ respectively.
- Google's Grumpy compiles Python to Go.
- MyHDL compiles Python to VHDL.
- Nuitka compiles Python into C++.

Library features

- Data Frame object for data manipulation with integrated indexing.
- Tools for reading and writing data between in-memory data structures and different file formats.
- Data alignment and integrated handling of missing data.
- Reshaping and pivoting of data sets.
- Label-based slicing, fancy indexing, and sub setting of large data sets.
- Data structure column insertion and deletion.

- Group by engine allowing split-apply-combine operations on data sets.
- Data set merging and joining.
- Hierarchical axis indexing to work with high-dimensional data in a lower-dimensional data structure.
- Time series-functionality: Date range generation and frequency conversion, moving window statistics, moving window linear regressions, date shifting and lagging.
- Provides data filtration.

CONCLUSION

In conclusion, the application of blockchain technology in digital certificate fraud detection represents a pivotal step toward fortifying the reliability and security of credentialing systems. By leveraging the decentralized and tamper-resistant characteristics of blockchain, the proposed system offers a robust solution to the prevalent issue of certificate fraud. The innovative approach of storing digital certificates on a blockchain not only prevents unauthorized alterations but also establishes a transparent and traceable ledger for seamless verification by authorized entities. The integration of smart contracts automates the comparison process, expediting the identification of fraudulent elements and streamlining the overall certificate validation. This system not only addresses immediate challenges posed by certificate fraud but sets a new standard for secure and transparent digital credential management. Furthermore, by prioritizing data privacy through advanced cryptographic techniques and adhering to compliance standards, the proposed system ensures that sensitive information remains accessible only to authorized parties. As we navigate an increasingly digital landscape, this blockchain-based solution stands as a testament to the potential of emerging technologies in safeguarding the integrity of crucial documentation and fostering trust in diverse industries.

REFERENCE

1. Ostapowicz, M., & Żbikowski, K. (2020, January). Detecting fraudulent accounts on blockchain: a supervised approach. In International Conference on Web Information Systems Engineering (pp. 18-31). Springer, Cham.

2. S. Daliri, "Using Harmony Search Algorithm in Neural Networks to Improve Fraud Detection in Banking System," (in English), Computational Intelligence and Neuroscience, Article vol. 2020, p. 5, Feb 2020, Art. no. 6503459.

3. S. M. Darwish, "An intelligent credit card fraud detection approach based on semantic fusion of two classifiers," (in English), Soft Computing, Article vol. 24, no. 2, pp. 1243-1253, Jan 2020.

4. Ruttala sailusha, Ramesh, V. Gnaneshwar, G.Ramakoteswara Rao, "Credit card fraud detection using machine learning", International Conference on Intelligent Computing and Control Systems (ICICCS 2020), IEEE.

5. Yu B, Wright J, Nepal S. Establishing Trust in the Internet of Things Ecosystem Using Blockchain. IEEE Cloud Computing, vol. 4, pp. 12-23, 2018.

6. Heta Naik, Prashasti Kanikar, "Credit Card Fraud Detection based on Machine Learning

Algorithms", International Journal of Computer Applications, 2019

7. Ntirogiannis, Konstantinos, Basilis Gatos, and Ioannis Pratikakis, "A Performance Evaluation Methodology for Historical Document Image Binarization." : 1-1, 2017.

8. A. Kumar and G. Gupta, “Fraud Detection in Online Transactions Using Supervised Learning Techniques,” in Towards Extensible and Adaptable Methods in Computing, S. Chakraverty, A. Goel, and S. Misra, Eds. Singapore: Springer Singapore, 2018.

9. N.K. Dumpeti, R. Kavuri, A framework to manage smart educational certificates and thwart forgery on a permissioned blockchain, Mater. Today Proc. (2021),

10. Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu, Hongbo Zhu. Blockchain for the IoT and industrial IoT, A review. Internet of Things. vol. 10, pp. 11- 13, 2020.