A

Major Project

On

BLOCKCHAIN BASED AUTONOMOUS NOTARIZATION SYSTEM USING NATIONAL eID CARD

(Submitted in partial fulfillment of the requirements for the award of Degree)

BACHELOR OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

V.Madhurima	(217R1A0563)
N.KalyanReddy	(217R1A0538)
A.AdarshReddy	(217R1A0502)

Under the Guidance of

Dr. K. MAHESWARI

(Associate Professor)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

(Accredited by NAAC, NBA, Permanently Affiliated to JNTUH, Approved by AICTE, New Delhi)

Recognized Under Section 2(f) & 12(B) of the UGCAct.1956,

Kandlakoya (V), Medchal Road, Hyderabad-501401.

April, 2025.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CMR
TECHNICAL CAMPUS
EXPLORE TO INVENT

CERTIFICATE

This is to certify that the project entitled "**BLOCKCHAIN BASED AUTONOMOUS NOTARIZATION SYSTEM USING NATIONAL eID CARD"** being submitted by **V.Madhurima (217R1A0563), N.Kalyan Reddy (217R1A0538) & A.Adarsh Reddy (217R1A0502)** in partial fulfillment of the requirements for the award of the degree of B.Tech in Computer Science and Engineering to the Jawaharlal Nehru Technological University Hyderabad, during the year 2024-25.

The results embodied in this thesis have not been submitted to any other University or Institute for the award of any degree or diploma.

Dr. K. Maheswari
Associate Professor
INTERNAL GUIDE

Dr. Nuthanakanti Bhaskar
HoD

Dr. A. Raji Reddy
DIRECTOR

Signature of External Examiner

Submitted for viva voice Examination held on ____________________

ACKNOWLEDGEMENT

We take this opportunity to express our gratitude to the people who have been instrumental in the successful completion of this project, we take this opportunity to express our profound gratitude and deep regard to our guide **Dr. K. Maheswari,** Associate Professor for her exemplary guidance, monitoring and constant encouragement throughout the project work. The blessing, help and guidance given by her shall carry us a long way in the journey of life on which we are about to embark.

We take this opportunity to extend our heartfelt appreciation to the Project Review Committee (PRC) Coordinators—**Dr. K. Maheswari, Dr. J. Narasimharao, Ms. K. Shilpa, and Mr. K. Ranjith Reddy**—for their unwavering support, insightful guidance, and valuable inputs, which played a crucial role in steering this project through its various stages.

Our sincere appreciation also goes to **Dr. Nuthanakanti Bhaskar**, Head, for his encouragement and continuous support in ensuring the successful completion of our project.

We are deeply grateful to **Dr. A. Raji Reddy**, Director, for his cooperation throughout the course of this project. Additionally, we extend our profound gratitude to Sri. **Ch. Gopal Reddy**, Chairman, Smt. **C. Vasantha Latha**, Secretary and Sri. **C. Abhinav Reddy**, Vice-Chairman, for fostering an excellent infrastructure and a conducive learning environment that greatly contributed to our progress.

We also acknowledge and appreciate the guidance and assistance provided by the faculty and staff of **CMR Technical Campus**, whose contributions have been invaluable in bringing this project to fruition.

Lastly, we sincerely thank our families for their unwavering support and encouragement. We also extend our gratitude to the teaching and non-teaching staff of CMR Technical Campus for their guidance and assistance. Their contributions, along with the support of everyone who helped directly or indirectly, have been invaluable in the successful completion of this project.

V.Madhurima (217R1A0563)
N.Kalyan Reddy (217R1A038)
A.Adarsh Reddy (217R1A0502)

VISION AND MISSION

INSTITUTE VISION:

To Impart quality education in serene atmosphere thus strive for excellence in Technology and Research.

INSTITUTE MISSION:

1. To create state of art facilities for effective Teaching- Learning Process.

2. Pursue and Disseminate Knowledge based research to meet the needs of Industry & Society.

3. Infuse Professional, Ethical and Societal values among Learning Community.

DEPARTMENT VISION:

To provide quality education and a conducive learning environment in computer engineering that foster critical thinking, creativity, and practical problem-solving skills.

DEPARTMENT MISSION:

1. To educate the students in fundamental principles of computing and induce the skills needed to solve practical problems.

2. To provide State-of-the-art computing laboratory facilities to promote industry institute interaction to enhance student's practical knowledge.

3. To inculcate self-learning abilities, team spirit, and professional ethics among the students to serve society.

ABSTRACT

This project is titled as “Blockchain Based Autonomous Notarization System Using National eID card”. In an era where digital transactions and legal agreements are increasingly prevalent, the need for secure, transparent, and efficient notarization systems has never been greater. This project presents a novel approach to notarization using blockchain technology, integrated with national electronic ID (eID) cards. The proposed system, termed the Blockchain Based Autonomous Notarization System (BANOS), leverages the immutability and transparency of blockchain to provide a decentralized and tamper proof mechanism for notarizing documents. The BANOS system utilizes national eID cards to authenticate users, ensuring that only verified individuals can initiate notarization processes. Once authenticated, users can submit documents for notarization, which are then recorded on a blockchain ledger. Each notarized document is hashed and stored on the blockchain, creating a verifiable and immutable record that can be accessed by relevant parties for validation. Key benefits of the BANOS system include enhanced security through cryptographic hashing and decentralized storage, reduced risk of fraud, and increased efficiency by automating the notarization process. By integrating with national eID systems, the solution ensures compliance with regulatory standards and provides a robust identity verification mechanism. This approach not only streamlines the notarization process but also establishes a new standard for digital trust and document integrity in the digital age. The project discusses the system's architecture, implementation details, and potential impacts on the future of notarization services.

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

1. INTRODUCTION

1. INTRODUCTION

The project, titled "Blockchain Based Autonomous Notarization System Using National eId Card," In today’s digital landscape, the demand for secure, efficient, and reliable document authentication systems is greater than ever. Traditional notarization processes often involve time-consuming procedures, physical presence, and high operational costs, which hinder accessibility and efficiency. To address these challenges, this project proposes a Blockchain-Based Autonomous Notarization System (BANS) that leverages blockchain technology and National eId Cards to create a secure, decentralized, and tamper-proof platform for document notarization.

The system enables users to upload documents through a secure web interface, where their identity is verified using digital signatures and biometric authentication embedded in their Eid cards. Once authenticated, the document is encrypted, timestamped, and a unique hash is stored on the blockchain, providing immutable proof of the document’s existence and integrity. By eliminating the need for in-person verification and automating the process, BANS enhances security, builds trust, reduces costs, and significantly improves the efficiency and accessibility of the notarization process in the digital age.

1.1 PROJECT PURPOSE

The purpose is to eliminate traditional notarization delays, costs, and physical presence requirements. It aims to offer a faster, more secure, and accessible solution through automation.

National eID cards, on the other hand, provide a secure and standardized means of verifying the identity of individuals. By integrating eID systems with blockchain, the notarization process can be streamlined while maintaining high standards of security and compliance.By using blockchain and Eid, it enhances trust, privacy, and efficiency in document verification.

1.2 PROJECT FEATURES

This project incorporates several key features that define its core functionality:

Digital Identity Verification via National eID: Authenticates users securely using government-issued electronic ID cards. Ensures that only legitimate individuals can notarize documents, providing legal validity and non-repudiation. Key Functions are two-factor authentication (PIN + biometric or card), digital signing with government-backed certificates.

Tamper-Proof Document Notarization via Blockchain: Stores the hash of the document and digital signature on the blockchain, ensuring the notarization cannot be altered or deleted. Provides a transparent, immutable, and verifiable record of notarization. Key Functions are generates SHA-256 hash of the uploaded document, writes notarization data to the blockchain (timestamp, user ID hash, signature hash) and enables public or permissioned verification.

Autonomous Smart Contract-Based Workflow: Automates the notarization process using smart contracts, removing the need for manual verification by a third-party notary. Speeds up processes, reduces cost, and eliminates human errors or fraud. Key Functions are automatically validates digital signatures, executes notarization logic and logs transactions and provides real-time status updates and verifiability.

2. LITERATURE SURVEY

1.LITERATURE SURVEY

A literature survey provides a comprehensive overview of existing research, methodologies, and technologies relevant to the proposed Blockchain Based Autonomous Notarization System (BANOS). This section explores previous work in blockchain technology, electronic ID (eID) systems, and digital notarization to establish a foundation for understanding the current state of the field and identifying gaps that the BANOS system aims to address.

The process of notarization, which traditionally involves certifying the authenticity of documents by a public notary, has long been a cornerstone of legal and administrative systems. However, with growing demand for digitization, transparency, and trustless environments, the conventional notarization system has come under scrutiny for its inefficiency, susceptibility to fraud, and heavy dependency on physical presence. In this context, blockchain technology presents a transformative opportunity to reinvent notarization systems by leveraging decentralized, immutable, and transparent digital ledgers. The integration of blockchain with national electronic identification (eID) systems can further enhance the security, credibility, and usability of digital notarization processes, particularly in public sector applications.

The concept of digital notarization using blockchain has been widely explored in academic and industry research. Early works have focused on the use of blockchain to timestamp documents, ensuring their integrity and proving their existence at a certain point in time. For instance, the work by Azaria et al. (2016) on MedRec demonstrated the use of blockchain for securing medical records, showing how timestamps and immutability can enforce trust in digital systems. Similar principles have been adapted for notarization, where a cryptographic hash of a document is stored on-chain, providing proof of integrity without revealing the content. This concept has matured over time, evolving into more sophisticated notarization frameworks that include smart contracts for automating legal workflows.

A key innovation in modern digital notarization systems is the use of *smart contracts*, programmable code that executes on the blockchain when predetermined conditions are met. Smart contracts enable autonomous verification and approval of notarization requests without human intervention. Projects like OpenLaw and Ubiquity have experimented with legal automation on the Ethereum blockchain, proving that legal documents can be both machine-readable and self-executing.

The integration of smart contracts into notarization processes ensures consistency, auditability, and efficiency, significantly reducing the need for manual validation and physical signatures.

Another important development in this space is the advent of national eID systems, which provide a secure and verifiable digital identity to citizens. Countries such as Estonia, Belgium, and India have deployed electronic identification infrastructure to support e-governance. Estonia’s e-Residency program, for example, allows users to digitally sign documents using a cryptographic key stored in a government-issued ID card. Similarly, India’s Aadhaar-based eKYC services have streamlined digital identity verification in banking and other sectors. When integrated with blockchain, national eID cards serve as strong digital identities that can authenticate users securely without the risk of impersonation or forgery. This dual approach of using eID for identity verification and blockchain for notarization ensures a highly secure and transparent system.

Recent studies have emphasized the importance of data privacy and regulatory compliance in blockchain-based notarization systems. GDPR in the European Union, for example, imposes strict rules about personal data handling, including the right to be forgotten. This presents a challenge for public blockchains where data is immutable and permanent. Several approaches have been proposed to tackle this, including off-chain storage, zero-knowledge proofs, and permissioned blockchains. By storing only hashed references on-chain and keeping sensitive data off-chain, systems can maintain regulatory compliance while leveraging blockchain’s security features. Hyperledger Fabric, a permissioned blockchain framework, has been adopted in some government-led projects to balance transparency and privacy.

From a technical perspective, various blockchain platforms have been evaluated for notarization applications. Ethereum, due to its robust smart contract capabilities and wide developer support, has been a popular choice. However, its public nature and high transaction fees have led researchers to consider alternatives like Hyperledger Fabric, Corda, and Tezos. These platforms offer greater control over data access and are often more suitable for enterprise or governmental use cases.

Additionally, interoperability between blockchain and eID systems is a critical aspect that is being addressed through APIs, digital signature standards, and middleware solutions. For example, the integration of PKI (Public Key Infrastructure) with blockchain ensures that digital signatures from eID cards can be validated across systems securely.

Several pilot projects and real-world implementations support the feasibility of a blockchain-based notarization system. In 2018, the government of Georgia partnered with Bitfury to implement blockchain land registry services. Similarly, Sweden's Lantmäteriet tested blockchain for property transactions. These projects have demonstrated reduced processing times, increased security, and greater trust among stakeholders. Academic institutions have also contributed by exploring prototype implementations and performance evaluations. A 2020 study by the IEEE proposed a blockchain-based notarization architecture that integrated biometric authentication and demonstrated improvements in both security and user trust.

In recent years, the convergence of digital identity systems and blockchain technology has gained increased attention from governments, international organizations, and private enterprises. One of the key drivers behind this trend is the rapid evolution of digital services and the corresponding need for secure, verifiable, and efficient identity authentication mechanisms. Traditional digital signature systems, while effective, are often siloed and lack interoperability across platforms and jurisdictions. Blockchain offers a decentralized approach that ensures tamper-proof audit trails and real-time verification, both of which are critical for high-trust applications like document notarization. When combined with national eID systems that provide cryptographically secure identification, the result is a powerful infrastructure capable of supporting autonomous, legally sound notarization services at scale.

An important aspect of blockchain-based notarization is its decentralized trust model, which eliminates the need for intermediaries such as notaries or centralized authorities. This decentralization not only reduces operational costs but also minimizes the risk of corruption, fraud, and human error. Research has shown that by using distributed consensus protocols, notarized records can be validated by multiple nodes in the network, ensuring higher levels of trust and security. Furthermore, blockchain’s append-only structure guarantees that once a document is notarized, its history remains permanently recorded, accessible, and verifiable. This feature is particularly useful in sectors like real estate, legal contracts, academic certifications, and government records, where document integrity is paramount.

Another promising direction being explored in current literature is the integration of biometric authentication with eID and blockchain systems. Biometric data such as fingerprints or facial recognition can add an extra layer of security to ensure that the person initiating the notarization process is indeed the rightful owner of the eID card. Combined with multi-factor authentication mechanisms, such systems can significantly reduce identity fraud. However, these innovations also raise concerns about data protection and privacy. To address this, recent research emphasizes the use of decentralized identity (DID) standards and self-sovereign identity (SSI) frameworks, which allow users to control their personal information and share only the minimum required data for any transaction.

Moreover, recent literature highlights the need for regulatory harmonization and standardization to fully integrate blockchain notarization systems into legal frameworks. While some countries have taken progressive steps—such as Estonia and the United Arab Emirates—others are still in the early stages of exploring legal recognition of blockchain-based documents. The International Organization for Standardization (ISO) and World Economic Forum (WEF) have called for collaborative efforts to define global standards for digital identities and blockchain governance. This includes setting parameters for smart contract validation, document authenticity, and interoperability with existing legal infrastructure.

There is also growing academic interest in evaluating the performance and scalability of blockchain-based notarization systems. As document volumes increase, especially in government and enterprise applications, the blockchain infrastructure must be capable of handling large-scale data without compromising speed or security. Layer-2 scaling solutions, such as sidechains and state channels, have been proposed to address these limitations. Additionally, hybrid architectures that combine private (permissioned) and public (permissionless) blockchains are being explored to balance transparency, privacy, and control. For example, sensitive data can be processed on a private chain while the hash of the transaction is anchored on a public chain to ensure immutability.

Interdisciplinary research is also shedding light on the *socioeconomic impact* of blockchain-based notarization. By enabling citizens to notarize documents remotely using their national eID cards, these systems can significantly enhance accessibility and inclusivity, particularly for rural and underserved populations.

They can also reduce bureaucratic bottlenecks, enhance cross-border document validation, and foster digital trust in e-governance platforms. For developing countries, such technology offers a leapfrogging opportunity to build transparent and corruption-resistant public institutions.

In conclusion, the literature strongly supports the viability of a Blockchain-Based Autonomous Notarization System Using National eID Cards. The convergence of blockchain technology, smart contracts, and national eID infrastructure presents a robust solution to the longstanding issues of inefficiency, fraud, and lack of transparency in traditional notarization processes. By providing immutable records, autonomous verification, and secure digital identity, such a system can significantly enhance trust and efficiency in both public and private sectors. Future research should focus on scalability, interoperability, and legal integration to fully realize the potential of blockchain-based notarization on a national and global scale.

1.1 REVIEW OF RELATED WORK

The digitization of government services and legal procedures has significantly accelerated in recent years, driven by advancements in blockchain technology and the widespread deployment of national electronic identification (eID) systems. The convergence of these technologies offers a promising foundation for building autonomous notarization systems that are secure, transparent, and legally recognized. This section reviews the existing literature and technologies in four primary areas: blockchain in notarization, digital identity systems, integration of eID in public services, and decentralized applications for legal documentation.

1. Blockchain in Notarization

Blockchain has been widely recognized as a transformative technology for notarization due to its inherent properties of immutability, decentralization, and transparency. Early work by [Ateniese et al., 2017] demonstrated how digital documents could be securely timestamped using cryptographic hashing and stored on public blockchain networks like Bitcoin. Their approach laid the groundwork for using blockchain as a notary-like service that does not rely on central authorities.

2. Digital Identity and National eID Systems

National eID systems are government-issued electronic identity frameworks that provide citizens with secure and verifiable credentials. These systems are designed to facilitate authentication, digital signing, and secure access to e-government services. Estonia's eID card system is widely cited as a leading example of national digital identity, supporting services such as online voting, tax filing, and digital prescriptions [Pappel & Kalvet, 2018].

3. eID Integration with Blockchain Systems

Integrating national eID with blockchain-based notarization presents both opportunities and challenges. While eID ensures that identities are legally verifiable, integrating them into decentralized systems without compromising user privacy or introducing central points of failure is complex. Hybrid approaches that combine on-chain hash storage with off-chain identity verification have been proposed to address these concerns.

4. Autonomous Notarization and Legal Validity

The notion of “autonomous” or “self-executing” notarization systems via smart contracts has been studied in various contexts. Smart contracts can perform automated checks, store timestamps, and trigger events when certain conditions are met. In the legal field, projects like OpenLaw and Kleros have explored the potential of using blockchain-based smart contracts to create legally enforceable agreements.

However, legal enforceability remains a challenge. While documents on the blockchain are immutable, courts may require additional proofs, such as verified identities and certified timestamps. This is where integration with national eID becomes crucial. By tying smart contracts and notarized documents to eID-signed inputs, legal systems can more easily validate their authenticity.

5. Summary and Research Gap

To summarize, the integration of blockchain with digital identity systems—particularly national eID—is a promising frontier in the field of digital notarization. Existing research has explored blockchain notarization, smart contracts, and decentralized identity solutions. National eID systems provide the legal grounding needed to make blockchain notarization acceptable in legal and governmental processes.

The review illustrates a strong research foundation in blockchain notarization, identity management, and smart contract automation. However, integrating these elements into a single, legally compliant system using national eID cards is still underexplored. The proposed system addresses this by leveraging blockchain's immutability, smart contracts' automation, and eID's legal identity framework to deliver a secure, efficient, and trustworthy digital notarization solution.

2.2 DEFINITION OF PROBLEM STATEMENT

This project aims to develop a Blockchain-Based Autonomous Notarization System (BANS) that modernizes the traditional notarization process by eliminating the need for physical presence and manual verification. Utilizing blockchain technology and National Eid Cards, the system ensures secure identity authentication, document integrity, and legal compliance. The objective is to provide a decentralized, efficient, and tamper-proof platform for notarizing documents, thereby enchancing accessibility, trust, and speed in official documentation processes.

2.3 EXISTING SYSTEM

In the existing system the current notarization system is predominantly manual and requires the physical presence of both the document holder and a licensed notary. It involves paper-based verification, handwritten signatures, and in-person identity checks, making the process time-consuming, costly, and often inconvenient. Additionally, the existing system lacks strong security measures, as physical documents are prone to loss, forgery, or tampering. There is minimal use of automation or digital identity verification, and storage of notarized records is typically centralized, making them vulnerable to unauthorized access or data breaches.

This traditional approach fails to meet the growing demand for remote, fast, and secure document verification in the digital age.

Limitations of Existing System

Despite significant advancements in both blockchain technology and national electronic identity (eID) systems, current implementations of blockchain-based notarization systems face several limitations. These disadvantages hinder their widespread adoption and practical deployment in real-world legal and governmental scenarios. Below are the key drawbacks of existing systems:

- Lack of Strong Identity Verification: Many existing blockchain-based notarization platforms allow users to create and verify documents using cryptographic keys without binding them to a verifiable legal identity. This introduces challenges such as:

  Anonymity and Impersonation Risks: Users can remain pseudonymous, making it difficult to legally validate who signed or submitted a document.

  Lack of Legal Recognition: In many jurisdictions, notarized documents must be tied to verifiable identities to hold up in court or be accepted by government institutions.

- Fragmented Integration with eID Systems: While national eID systems are robust on their own, their integration with blockchain platforms is still in its infancy. Existing efforts are often:

  Country-Specific: Most blockchain-eID integrations are tailored to a single country’s infrastructure (e.g., Estonia, Belgium), lacking cross-border interoperability.

  Not Fully Automated: Many implementations require manual verification steps or third-party intermediaries, which diminishes the benefit of automation promised by blockchain.

- Privacy Concerns and Data Exposure: Storing notarized documents or identity-related metadata directly on a public blockchain can raise serious privacy concerns:

  Irreversible Exposure: Once data is on a public blockchain, it cannot be removed or modified. If sensitive personal information is exposed, it can lead to long-term privacy violations.

  Non-Compliance with Privacy Laws: Solutions that do not separate on-chain and off-chain data risk violating privacy laws like the General Data Protection Regulation (GDPR), which mandates user data control and deletion rights.

2.4 PROPOSED SYSTEM

The proposed system, Blockchain-Based Autonomous Notarization System (BANS), is a secure and decentralized platform that allows users to notarize documents online using National eID Cards. It verifies the user's identity through digital signatures and biometric authentication, ensuring legal compliance and trust. Once verified, the system encrypts the document, generates a unique hash, and stores it on a blockchain, creating an immutable, tamper-proof record. A digitally signed certificate is then issued as proof of notarization. By eliminating the need for physical presence and manual intervention, BANS offers a faster, cost-effective, and highly secure alternative to traditional notarization methods.

Advantages of the Proposed System:

The proposed system significantly improves upon the existing approaches by addressing key limitations:

- Enhanced Security: Blockchain Immutability: Once notarized, documents can't be altered or tampered with. eID-Based Authentication: Only legitimate users can access or notarize documents using secure national eID credentials.

- Legal Validity & Trust: Digital signatures through national eID cards are often legally recognized. Blockchain timestamps can serve as verifiable proof of time and origin of a document.

- Automation & Efficiency: No need to visit notary offices physically. Smart contracts can automate verification and notarization, reducing manual processes and wait times.

- Cost Reduction: Eliminates intermediaries (notary offices, legal clerks). Reduces paper-based processes and administrative overhead.

- Transparency & Auditability: Every transaction (notarization) is logged on-chain and can be traced without revealing confidential details. Enables easy auditing and verification by third parties.

2.5 OBJECTIVES

- To Develop a Secure and Tamper-Proof Notarization System – Utilize blockchain technology to ensure document integrity and immutability. Prevent unauthorized changes and document forgery through cryptographic hashing.

- To Integrate National eID for User Authentication – Leverage the national eID infrastructure to authenticate users securely. Ensure only authorized individuals can notarize, access, or verify documents.

- To Automate the Notarization Process Using Smart Contracts – Replace manual notarization tasks with automated workflows. Enable real-time validation, timestamping, and certification of documents.

- To Provide a Decentralized and Transparent Notarization Platform – Eliminate reliance on a centralized notary authority. Promote transparency, traceability, and trust among users and authorities.

- To Enable 24/7 Access to Notarization Services –Build a platform that is always available regardless of working hours or geographic location. Support remote and cross-border notarization for individuals and organizations.

2.6 HARDWARE & SOFTWARE REQUIREMENTS

2.6.1 HARDWARE REQUIREMENTS:

Hardware interfaces specifies the logical characteristics of each interface between the software product and the hardware components of the system. The following are some hardware requirements,

Processor	Intel Core i5
Hard disk	512 GB.
RAM	16 GB.

2.6.2 SOFTWARE REQUIREMENTS:

Software Requirements specifies the logical characteristics of each interface and software components of the system. The following are some software requirements,

Operating system	Windows 10
Language	Python
Back-End	Django
Frame Work	Tkinter

3. SYSTEM ARCHITECTURE & DESIGN

3.SYSTEM ARCHITECTURE & DESIGN

The system design for BANOS focuses on integrating blockchain technology with national electronic ID (eID) systems to create a secure, efficient, and scalable notarization platform. The design includes detailed specifications for hardware, software, and user interaction, ensuring that the system meets its goals of reliability, security, and user friendliness.

3.1 PROJECT ARCHITECTURE

This project architecture shows the procedure and illustrates a digital signature verification system using smart contracts and public key.

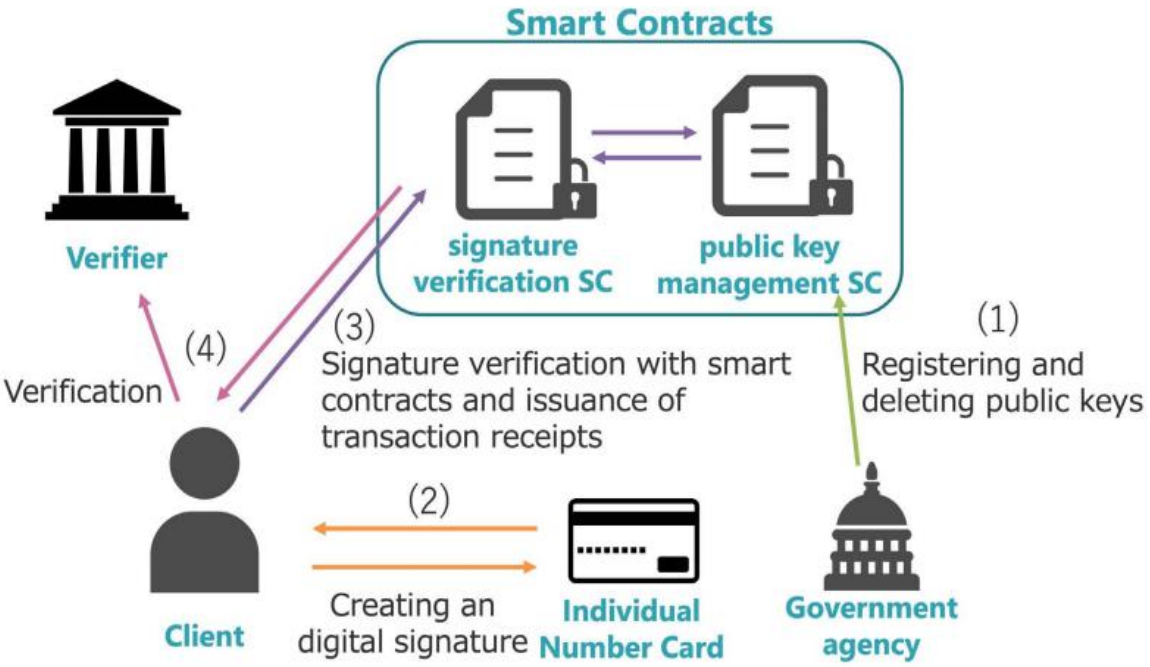

Smart Contracts
signature verification SC
public key management SC
Verifier
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Client
Creating an digital signature
Individual Number Card
Government agency

Figure 3.1: Project Architecture of Blockchain-Based Autonomous Notarization System Using National eID Card

3.2 DESCRIPTION

Government Agency: Registers and manages public keys. Registers or deletes public keys in the Public Key Management Smart Contract (SC). Ensures only valid, verified public keys are stored on the blockchain.

Client and Individual Number Card: The client creates a digital signature using their Individual Number Card (eID). The card generates a digital signature for the client. This signature will later be used for verification in the notarization process.

Smart Contracts : The system uses two key smart contracts:

- **Public Key Management SC**:
  Stores and manages public keys.
  Allows updates/deletions initiated by the government agency.
- **Signature Verification SC**:
  Verifies digital signatures using public keys stored in the Public Key Management SC.
  Issues transaction receipts upon successful verification.

The smart contracts interact with each other to fetch public keys and verify
signatures autonomously.

Verifier : Validates the client's identity and the authenticity of the transaction. Receives verification data from the client. Uses the Signature Verification SC to check the signature against registered public keys. Confirms the verification result back to the client.

3.3 DATA FLOW DIAGRAM

A Data Flow Diagram (DFD) is a graphical representation that illustrates how data flows within a system, showcasing its processes, data stores, and external entities. It is a vital tool in system analysis and design, helping stakeholders visualize the movement of information, identify inefficiencies, and optimize workflows.

A Data Flow Diagram comprises Four primary elements:

- External Entities: Represent sources or destinations of data outside the system.
- Processes: Indicate transformations or operations performed on data.
- Data Flows: Depict the movement of data between components.
- Data Stores: Represent where data is stored within the system.

These components are represented using standardized symbols, such as circles for processes, arrows for data flows, rectangles for external entities, and open-ended rectangles for data stores.

Benefits:

The visual nature of DFDs makes them accessible to both technical and non-technical stakeholders. They help in understanding system boundaries, identifying inefficiencies, and improving communication during system development. Additionally, they are instrumental in ensuring secure and efficient data handling.

Applications:

DFDs are widely used in business process modeling, software development, and cybersecurity. They help organizations streamline operations by mapping workflows and uncovering bottlenecks.

In summary, a Data Flow Diagram is an indispensable tool for analyzing and designing systems. Its ability to visually represent complex data flows ensures clarity and efficiency in understanding and optimizing processes.

Levels of DFD:

DFDs are structured hierarchically:

- Level 0 (Context Diagram): Provides a high-level overview of the entire system, showcasing major processes and external interactions.

- Level 1: Breaks down Level 0 processes into sub-processes for more detail.

- Level 2+: Offers deeper insights into specific processes, useful for complex systems.

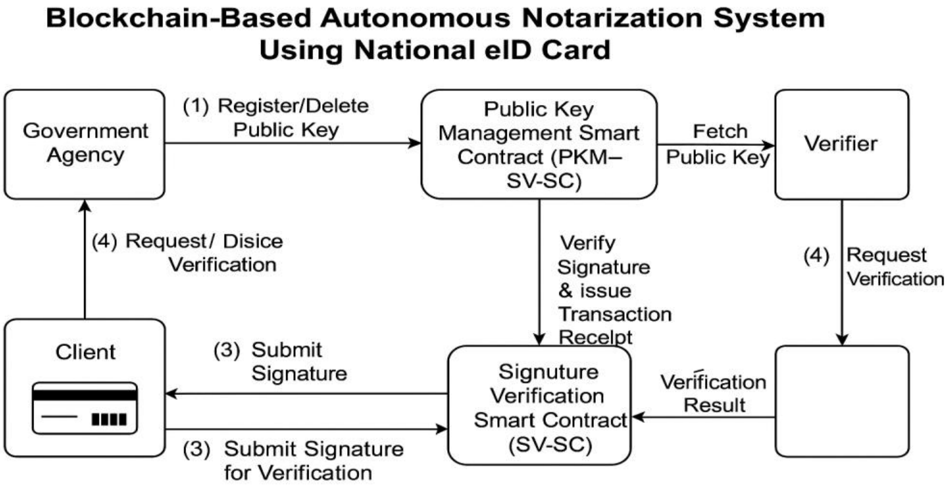

Blockchain-Based Autonomous Notarization System Using National eID Card
Government Agency
(1) Register/Delete Public Key
Public Key Management Smart Contract (PKM–SV-SC)
Fetch Public Key
Verifier
(4) Request/ Disice Verification
Verify Signature & issue Transaction Recelpt
(4) Request Verification
Client
(3) Submit Signature
Signuture Verification Smart Contract (SV-SC)
Verification Result
(3) Submit Signature for Verification

Figure 3.2: Dataflow Diagram of Blockchain-Based Autonomous Notarization System Using National eID Card

4. IMPLEMENTATION

4.IMPLEMENTATION

The implementation of the Blockchain-Based Autonomous Notarization System Using a National eID Card involves integrating smart contracts with a national identity system to enable secure and automated digital notarization. Public keys are registered and managed on a blockchain via a government-administered smart contract. Clients use their national eID cards to create digital signatures, which are then verified through another smart contract that cross-checks public keys and signature authenticity. A web-based interface allows clients to sign documents, verifiers to validate signatures, and government agencies to manage keys. The system ensures tamper-proof, transparent, and decentralized notarization without the need for manual intermediaries.

4.1 ALGORITHMS USED

Digital Signature Algorithm (DSA / ECDSA)

Enables clients to sign documents using their National eID card. Signature creation and verification.The client signs a document hash using their private key stored in the eID card. The smart contract verifies this signature using the associated public key.

Hashing Algorithm (SHA-256 or Keccak-256)

Generates a fixed-size hash from the input data (document). Document fingerprinting before signing. Signature verification inside smart contracts. Hashing ensures integrity and immutability.

Signature Verification Algorithm (ecrecover in Ethereum)

Reconstructs the signer's address from the digital signature. Smart contract uses ecrecover to check if the recovered address matches the stored public key.

Public Key Infrastructure (PKI) : Ensures secure key management by the government authority. Registering, revoking, and managing public keys on-chain. Trust anchor for the entire notarization process.

Smart Contract Logic (Custom Business Rules)

Defines the autonomous verification and notarization rules. Validating ownership of signatures. Recording notarization results on the blockchain. Ensuring only authorized entities can manage keys.

Together, these algorithms create a secure, tamper-proof, and fully automated notarization system that leverages blockchain's immutability and the trusted identity of national eID cards.

4.2 SAMPLE CODE

```
from django.shortcuts import render
from django.template import RequestContext
from django.contrib import messages
from django.http import HttpResponse
from django.core.files.storage import
FileSystemStorage
import os
from datetime import date
import json
from web3 import Web3, HTTPProvider
import hashlib

global username, usersList, notaryList,
contract, web3

#function to call contract
def getContract():
    global contract, web3
    blockchain_address = 'http://127.0.0.1:9545'
    web3 =
Web3(HTTPProvider(blockchain_address))
    web3.eth.defaultAccount =

web3.eth.accounts[0]
```

```
    compiled_contract_path = 'Notary.json'
#Logistic contract file
    deployed_contract_address =
'0xb1fe285e049D8C29bec9Fb178AE8A6eFc5
202085' #contract address
    with open(compiled_contract_path) as file:
        contract_json = json.load(file)  # load
contract info as JSON
        contract_abi = contract_json['abi']  # fetch
contract's abi - necessary to call its functions
    file.close()
    contract =
web3.eth.contract(address=deployed_contract_
address, abi=contract_abi)
getContract()

def getUsersList():
    global usersList, contract
    usersList = []
    count =
contract.functions.getUserCount().call()
    for i in range(0, count):
        user =
contract.functions.getUsername(i).call()
        password =
contract.functions.getPassword(i).call()
        phone =
contract.functions.getPhone(i).call()
        email =
contract.functions.getEmail(i).call()
        address =
contract.functions.getAddress(i).call()

        usersList.append([user, password, phone,
email, address])

def getNotary():
    global notaryList, contract
    notaryList = []
    count =
contract.functions.getNotaryCount().call()
    for i in range(0, count):
        uname =
contract.functions.getOwner(i).call()
        fname =
contract.functions.getFilename(i).call()
        hashcode =
contract.functions.getHashcode(i).call()
        dd = contract.functions.getDate(i).call()
        signature =
contract.functions.getSignature(i).call()
        key = contract.functions.getKey(i).call()
        notaryList.append([uname, fname,
hashcode, signature, dd, key])

getUsersList()
getNotary()

def VerifyNotaryAction(request):
    if request.method == 'POST':
        global username, notaryList
        today = date.today()
        pin = request.POST.get('t1', False)
        filedata = request.FILES['t2'].read()
        filename = request.FILES['t2'].name
```

```
   hashcode=hashlib.sha256(filedata).hexdigest()
key=hashlib.sha256(pin.encode()).hexdigest()
           status = "Verification Failed"
           for i in range(len(notaryList)):
               nl = notaryList[i]
               if nl[2] == hashcode and nl[5] == key:
                   status = nl
                   break
           if status != "Verification Failed":
               output = '<table border=1
   align=center>'
               output+='<tr><th><font size=3
   color=black>Owner Name</font></th>'
               output+='<th><font size=3
   color=black>eID File Name</font></th>'
               output+='<th><font size=3
   color=black>Hashcode</font></th>'
               output+='<th><font size=3
   color=black>Signature</font></th>'
               output+='<th><font size=3
   color=black>Date</font></th>'
               output+='<th><font size=3
   color=black>Key</font></th></tr>'
               arr = status[3].split("$")
               output+='<tr><td><font size=3
   color=black>'+status[0]+'</font></td>'
               output+='<td><font size=3
   color=black>'+status[1]+'</font></td>'
               output+='<td><font size=3
   color=black>'+status[2][0:20]+'</font></td>'
               output+='<td><font size=3
   color=black>'+arr[0]+'</font></td>'


        output+='<td><font size=3
```

```
color=black>'+status[4]+'</font></td>'
            output+='<td><font size=3
color=black>'+status[5][0:20]+'</font></td></t
r>'
            output+='<tr><td><font size=3
color=black>Notary Text :
'+arr[1]+'</font></td></tr>'
            status = output
        context= {'data': status}
        return render(request,
'VerifierScreen.html', context)

def VerifyNotary(request):
    if request.method == 'GET':
       return render(request, 'VerifyNotary.html',
{})

def AddNotary(request):
    if request.method == 'GET':
       return render(request, 'AddNotary.html',
{})

def AddNotaryAction(request):
    if request.method == 'POST':
        global username, notaryList
        today = date.today()
        notary = request.POST.get('t1', False)
        pin = request.POST.get('t2', False)
        filedata = request.FILES['t3'].read()
        filename = request.FILES['t3'].name



hashcode =hashlib.sha256(filedata).hexdigest()
```

```
key=hashlib.sha256(pin.encode()).hexdigest()
            status = "none"
            for i in range(len(notaryList)):
                nl = notaryList[i]
                if nl[2] == hashcode:
                    status = "Your eID Card Alread
    exists"
                    break
            if status == "none":
                msg =
    contract.functions.RegisterHash(username,
    filename, hashcode, pin+"$"+notary,
    str(today), key).transact()
                tx_receipt =
    web3.eth.waitForTransactionReceipt(msg)
                notaryList.append([username, filename,
    hashcode, pin+"$"+notary, str(today), key])
                status = "Your notary details
    successfully saved in Blockchain using below
    details<br/>"+str(tx_receipt)
            else:
                status = "Error in saving Notary details"
            context= {'data': status}
            return render(request, 'AddNotary.html',
    context)

    def DeleteNotaryAction(request):
        if request.method == 'GET':
            global uname, contract, notaryList
            rid = request.GET['file']

    contract.functions.deleteKey(int(rid)).transact()

      nl = notaryList[int(rid)]
```

```
        nl[2] = "Delete"
        context= {'data': "Given notary key
deleted from Blockchain"}
        return render(request, 'UserScreen.html',
context)

def ViewNotary(request):
    if request.method == 'GET':
        global contract, notaryList, username
        output = '<table border=1 align=center>'
        output+='<tr><th><font size=3
color=black>Owner Name</font></th>'
        output+='<th><font size=3
color=black>eID File Name</font></th>'
        output+='<th><font size=3
color=black>Hashcode</font></th>'
        output+='<th><font size=3
color=black>Signature</font></th>'
        output+='<th><font size=3
color=black>Date</font></th>'
        output+='<th><font size=3
color=black>Key</font></th></tr>'
        for i in range(len(notaryList)):
            nl = notaryList[i]
            if nl[0] == username:
                arr = nl[3].split("$")
                output+='<tr><td><font size=3
color=black>'+nl[0]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[1]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[2][0:20]+'</font></td>'

    output+='<td><font size=3
```

```
color=black>'+arr[0]+'</font></td>'
            output+='<td><font size=3
color=black>'+nl[4]+'</font></td>'
            output+='<td><font size=3
color=black>'+nl[5][0:20]+'</font></td></tr>'
            output+='<tr><td><font size=3
color=black>Notary Text :
'+arr[1]+'</font></td></tr>'
        context= {'data': output}
        return render(request, 'UserScreen.html',
context)

def DeleteNotary(request):
    if request.method == 'GET':
        global contract, notaryList, username
        output = '<table border=1 align=center>'
        output+='<tr><th><font size=3
color=black>Owner Name</font></th>'
        output+='<th><font size=3
color=black>eID File Name</font></th>'
        output+='<th><font size=3
color=black>Hashcode</font></th>'
        output+='<th><font size=3
color=black>Signature</font></th>'
        output+='<th><font size=3
color=black>Date</font></th>'
        output+='<th><font size=3
color=black>Key</font></th>'
        output+='<th><font size=3
color=black>Delete Notary</font></th></tr>'
        for i in range(len(notaryList)):
            nl = notaryList[i]

         if nl[0] == username and nl[2] !=
"Delete":
                arr = nl[3].split("$")
                output+='<tr><td><font size=3
color=black>'+nl[0]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[1]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[2][0:20]+'</font></td>'
                output+='<td><font size=3
color=black>'+arr[0]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[4]+'</font></td>'
                output+='<td><font size=3
color=black>'+nl[5][0:20]+'</font></td>'
                output+='<td><a
href=\'DeleteNotaryAction?file='+str(i)+'\'><fo
nt size=3 color=black>Click
Here</font></a></td></tr>'
                output+='<tr><td><font size=3
color=black>Notary Text :
'+arr[1]+'</font></td></tr>'
        context= {'data': output}
        return render(request, 'UserScreen.html',
context)

def VerifierLoginAction(request):
    if request.method == 'POST':
        global username, usersList
        username = request.POST.get('t1', False)
        password = request.POST.get('t2', False)
        if username == 'admin' and password ==
'admin':

     context= {'data':"Welcome "+username}
```

```
            return render(request,
'VerifierScreen.html', context)
        else:
            context= {'data':'Invalid login details'}
            return render(request,
'VerifierLogin.html', context)

def VerifierLogin(request):
    if request.method == 'GET':
       return render(request, 'VerifierLogin.html',
{})

def index(request):
    if request.method == 'GET':
       return render(request, 'index.html', {})

def Login(request):
    if request.method == 'GET':
       return render(request, 'Login.html', {})

def Signup(request):
    if request.method == 'GET':
       return render(request, 'Signup.html', {})

def SignupAction(request):
    if request.method == 'POST':
        global contract, usersList
        username = request.POST.get('t1', False)
        password = request.POST.get('t2', False)
        contact = request.POST.get('t3', False)
        email = request.POST.get('t5', False)
        address = request.POST.get('t6', False)

     record = 'none'
```

```
  for i in range(len(usersList)):
            ul = usersList[i]
            if ul[0] == username:
                record = "exists"
                break
        if record == 'none':
            msg =
contract.functions.saveUser(username,
password, contact, email, address).transact()
            tx_receipt =
web3.eth.waitForTransactionReceipt(msg)
            usersList.append([username, password,
contact, email, address])
            context= {'data':'Signup process
completed and record saved in
Blockchain<br/>'+str(tx_receipt)}
            return render(request, 'Signup.html',
context)
        else:
            context= {'data':username+'Username
already exists'}
            return render(request, 'Signup.html',
context)

def LoginAction(request):
    if request.method == 'POST':
        global username, usersList
        username = request.POST.get('t1', False)
        password = request.POST.get('t2', False)
        status = 'none'
        for i in range(len(usersList)):
            ul = usersList[i]
```

```
 if ul[0] == username and ul[1] == password:

   status = 'success'
          break
      if status == 'success':
         context= {'data':"Welcome
"+username}
         return render(request,
'UserScreen.html', context)
      else:
         context= {'data':'Invalid login details'}
         return render(request,
'Login.html', context)
```

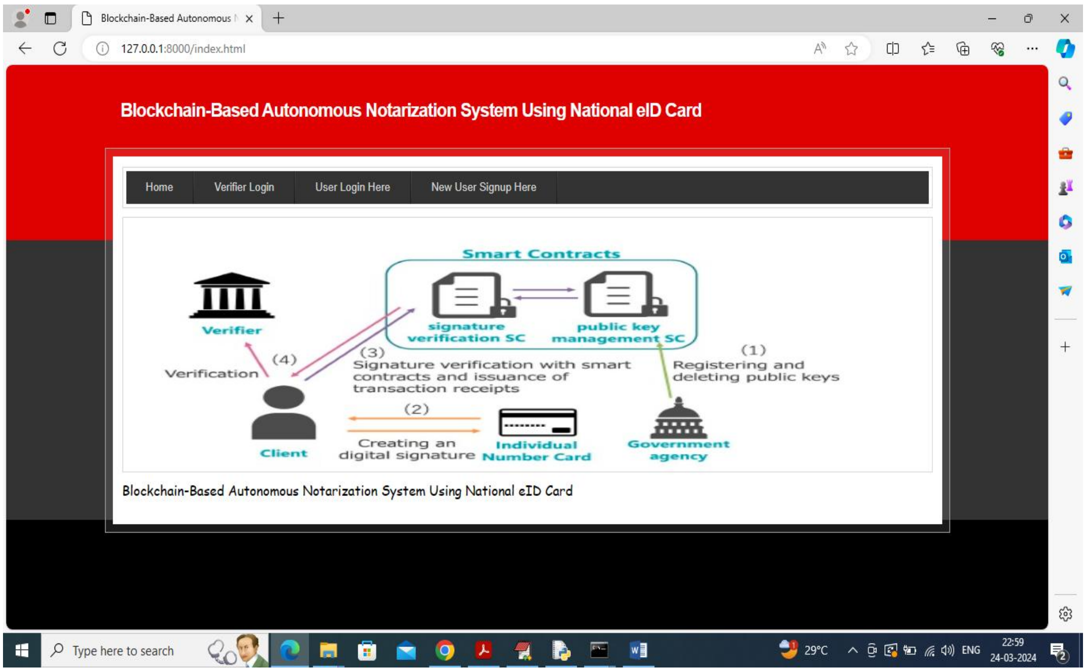
5.RESULTS & DISCUSSION

5.RESULTS & DISCUSSION

The following screenshots showcase the results of our project, highlighting key features and functionalities. These visual representations provide a clear overview of how the system performs under various conditions, demonstrating its effectiveness and user interface. The screenshots serve as a visual aid to support the project's technical and operational achievements.

5.1 GUI/Main Interface :

In below screen, click on ‘New User Sign up’ link .


Blockchain-Based Autonomous N
127.0.0.1:8000/index.html
Home
Verifier Login
User Login Here
New User Signup Here
Smart Contracts
signature verification SC
public key management SC
Verifier
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Creating an digital signature
Client
Individual Number Card
Government agency
Type here to search
29°C
ENG
22:59
24-03-2024

Blockchain-Based Autonomous Notarization System Using National eID Card

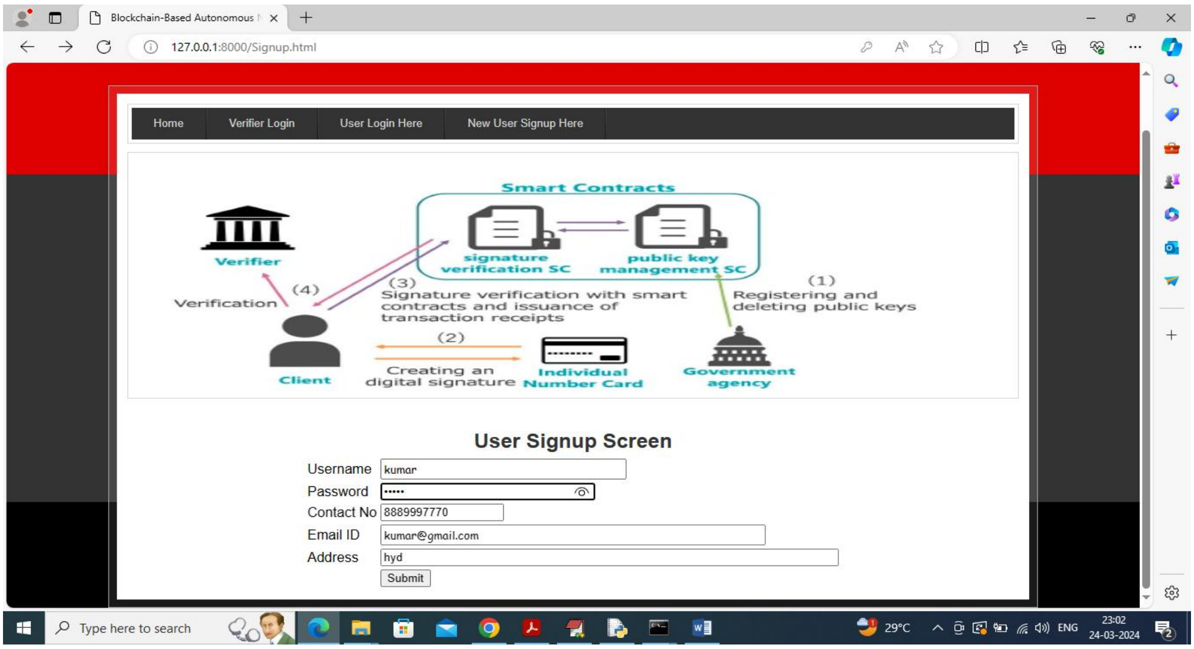
Blockchain-Based Autonomous Notarization System Using National eID Card

Figure 5.1 : GUI/Main Interface of Blockchain-Based Autonomous Notarization System Using National eID Card.

5.2 New User Sign Up :

In below screen, user is entering sign up details and then press the submit button.

New users can sign up with the application and all details (Username, Password, Contact No, Email ID, Address) will get saved in Blockchain.


Blockchain-Based Autonomous N
127.0.0.1:8000/Signup.html
Home
Verifier Login
User Login Here
New User Signup Here
Smart Contracts
signature verification SC
public key management SC
Verifier
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Creating an digital signature
Client
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:02
24-03-2024

User Signup Screen

Username	kumar
Password	•••••
Contact No	8889997770
Email ID	kumar@gmail.com
Address	hyd

Submit

Figure 5.2 : New User Sign Up image of Blockchain-Based Autonomous Notarization System Using National eID Card.

Now click on “User Login” link to get below page.

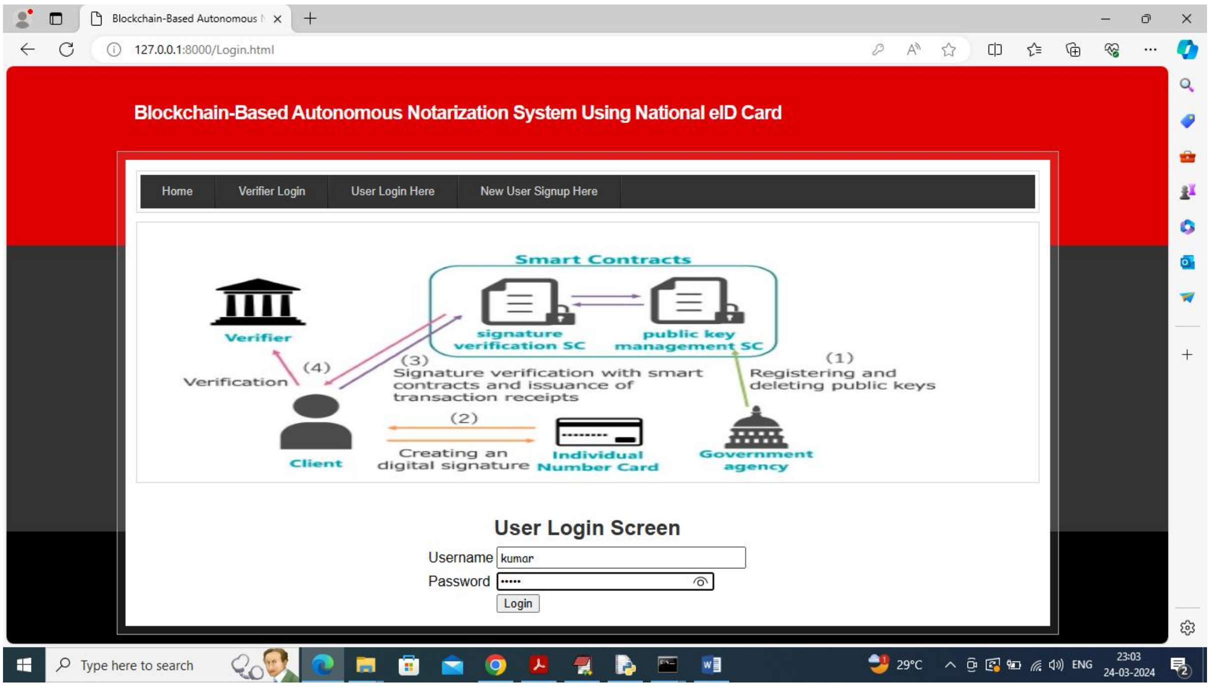
5.3 User Login:

1) In below screen, user can login with sign up details and after login user will perform below operations

2) Add Notary: user can create notary using pin no and eID file

3) Delete Notary: user can delete any existing notary details and keys

4) View Notary: using this module user can view notary on particular eID and pin no.



Blockchain-Based Autonomous Notarization System Using National eID Card

User Login Screen

Username kumar

Password •••••

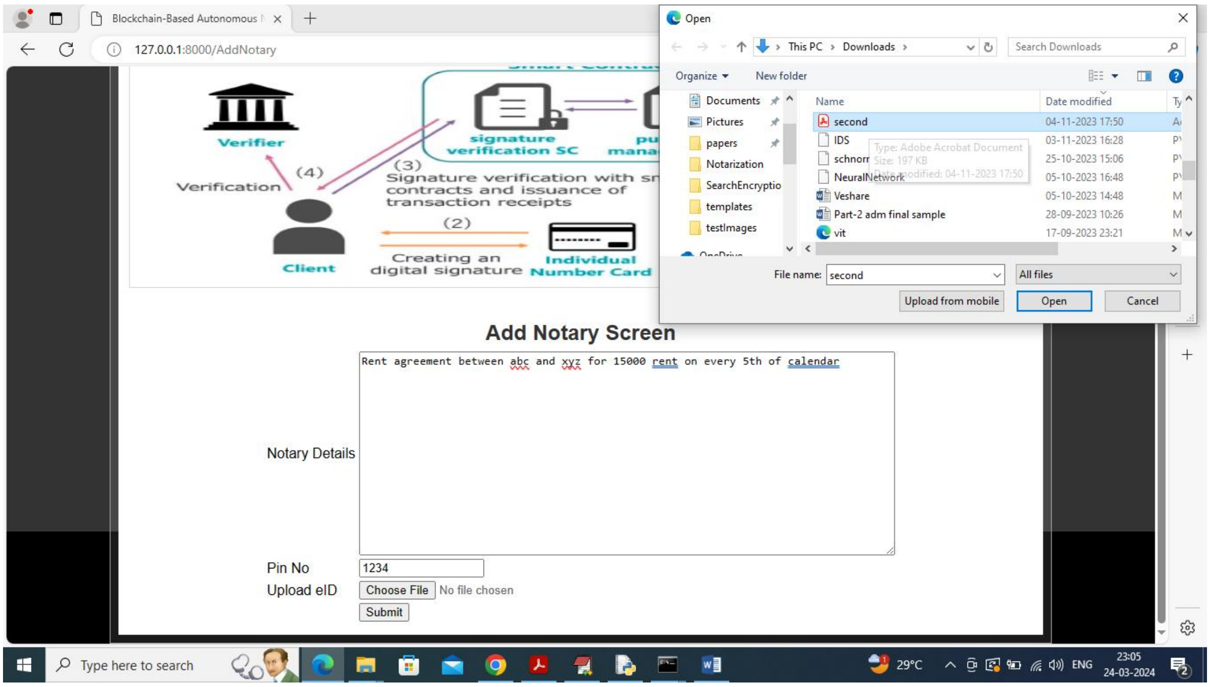
Blockchain-Based Autonomous N
127.0.0.1:8000/Login.html
Home
Verifier Login
User Login Here
New User Signup Here
Smart Contracts
signature verification SC
public key management SC
Verifier
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Creating an digital signature
Client
Individual Number Card
Government agency
Login
Type here to search
29°C
ENG
23:03
24-03-2024

Figure 5.3 : User Login of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen user is login and after login will get Welcome User with user name mentioned in the User Login screen.

5.4 Add Notary:

In above screen user can click on ‘Add Notarization’ link to create notary and will get below screen. below screen enter some notary text and then enter pin no and then select some eID document and then click on ‘Open’ and ‘Submit’ button to hash document and save all notary details to Blockchain and will get below output.



Add Notary Screen

Notary Details: Rent agreement between abc and xyz for 15000 rent on every 5th of calendar

Pin No: 1234

Upload eID: Choose File No file chosen

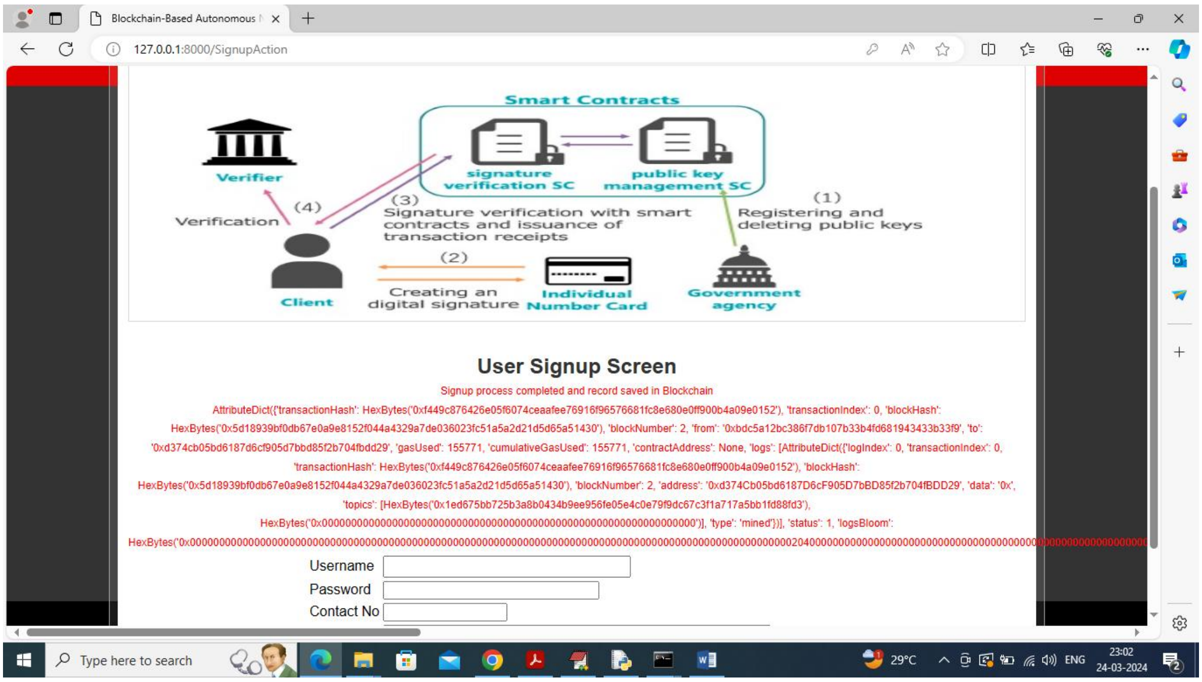
Submit

File name: second

Figure 5.4 : “Add Notary” of Blockchain-Based Autonomous Notarization System Using National eID Card.

5.5 Notary Details Saved In Blockchain :

In below screen, notary details saved in Blockchain and can see all transaction receipt.


Blockchain-Based Autonomous
127.0.0.1:8000/SignupAction
Smart Contracts
signature verification SC
public key management SC
Verifier
Verification
(4)
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Creating an digital signature
Client
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:02
24-03-2024

User Signup Screen

Signup process completed and record saved in Blockchain

```
AttributeDict({'transactionHash': HexBytes('0xf449c876426e05f6074ceaafee76916f96576681fc8e680e0ff900b4a09e0152'), 'transactionIndex': 0, 'blockHash':
HexBytes('0x5d18939bf0db67e0a9e8152f044a4329a7de036023fc51a5a2d21d5d65a51430'), 'blockNumber': 2, 'from': '0xbdc5a12bc386f7db107b33b4fd681943433b33f9', 'to':
'0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 155771, 'cumulativeGasUsed': 155771, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0, 'transactionIndex': 0,
'transactionHash': HexBytes('0xf449c876426e05f6074ceaafee76916f96576681fc8e680e0ff900b4a09e0152'), 'blockHash':
HexBytes('0x5d18939bf0db67e0a9e8152f044a4329a7de036023fc51a5a2d21d5d65a51430'), 'blockNumber': 2, 'address': '0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x',
'topics': [HexBytes('0x1ed675bb725b3a8b0434b9ee956fe05e4c0e79f9dc67c3f1a717a5bb1fd88fd3'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')], 'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000204000000000000000000000
```

Username

Password

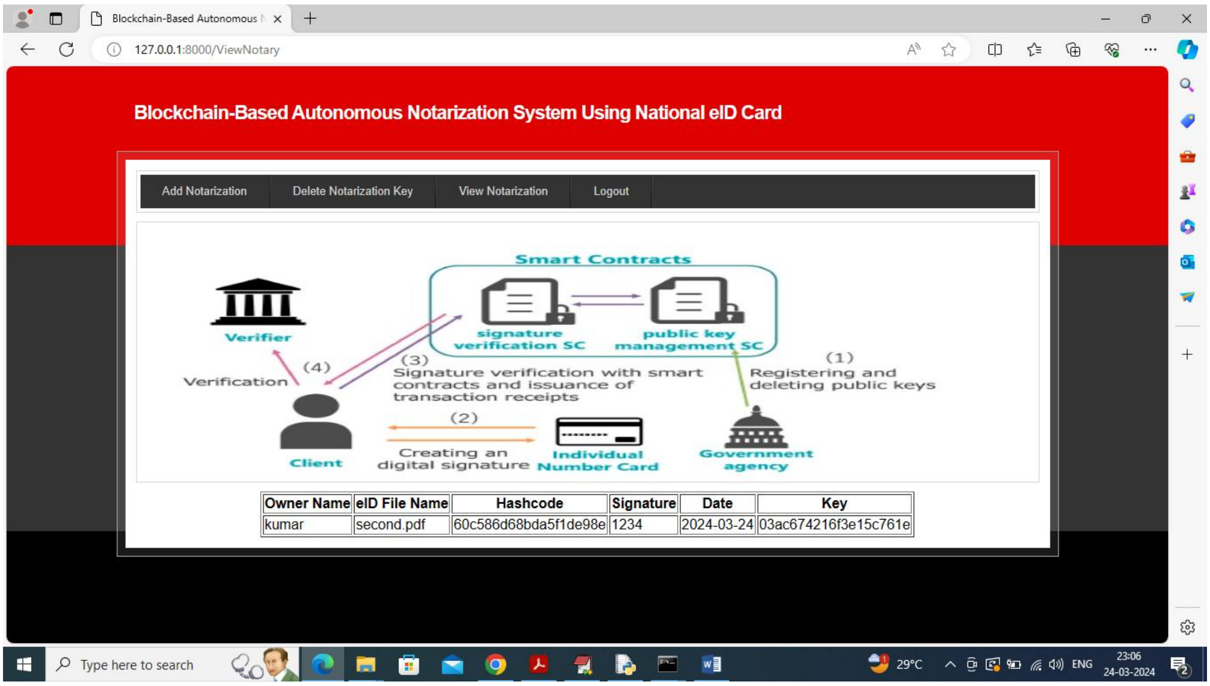
Contact No

Figure 5.5 : Notary Details Saved In Blockchain of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen in red colour text we got transaction receipt from Ethereum and for your understanding purpose we are displaying entire details instead of displaying transaction hash code. In above output we can see block no, transaction hash and many other details.

5.6 View Notary:

In below screen, click on ‘View Notarization’ link to view all existing created notary details with owner name, eID file name, hash code, signature, date and key.


Blockchain-Based Autonomous
127.0.0.1:8000/ViewNotary
Blockchain-Based Autonomous Notarization System Using National eID Card
Add Notarization
Delete Notarization Key
View Notarization
Logout
Smart Contracts
Verifier
signature verification SC
public key management SC
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
Client
(2)
Creating an digital signature
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:06
24-03-2024

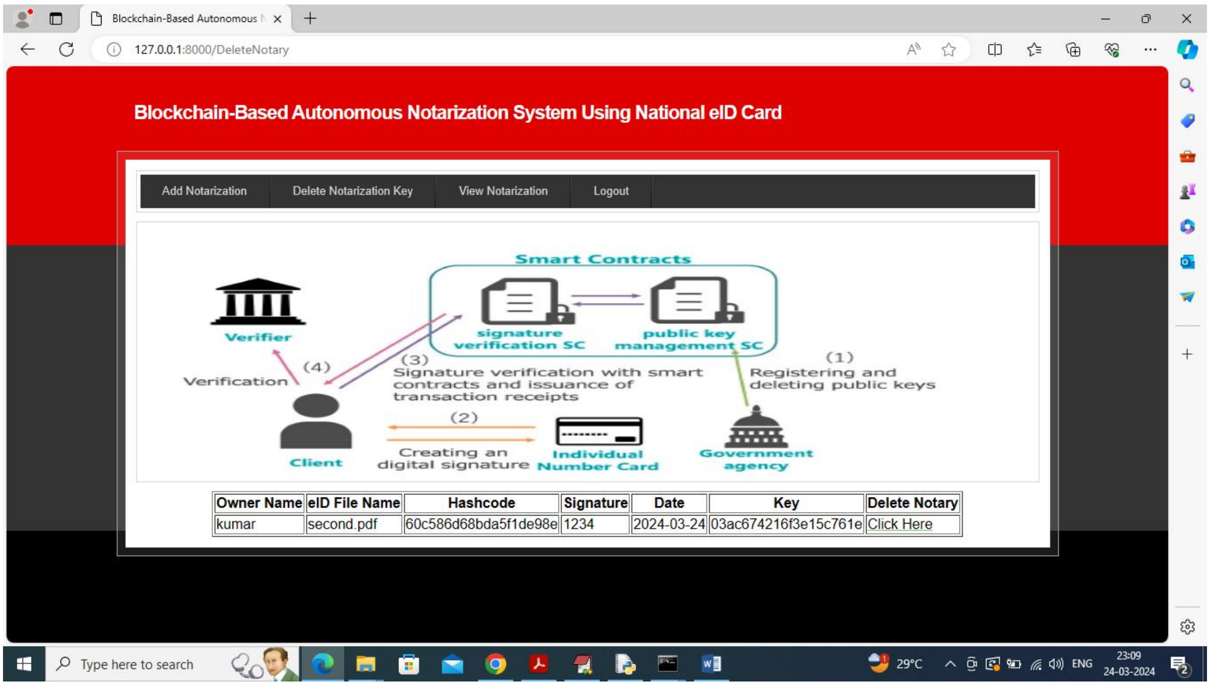
Owner Name	eID File Name	Hashcode	Signature	Date	Key
kumar	second.pdf	60c586d68bda5f1de98e	1234	2024-03-24	03ac674216f3e15c761e

Figure 5.6 : View Notary of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen user can view all notary details along with signature, key hash code and created fixed date. To delete notary and its key then click on ‘Delete Notarization key’ link to get below output.

5.7 Delete Notarization:

In below screen, a blockchain-based notary system interface showing a table of notarized files with details such as owner name, eID file name, hashcode, signature, date, unique key, and an option to delete each notary entry.


Blockchain-Based Autonomous N
127.0.0.1:8000/DeleteNotary
Blockchain-Based Autonomous Notarization System Using National eID Card
Add Notarization
Delete Notarization Key
View Notarization
Logout
Smart Contracts
signature verification SC
public key management SC
Verifier
Verification
(4)
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Client
Creating an digital signature
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:09
24-03-2024

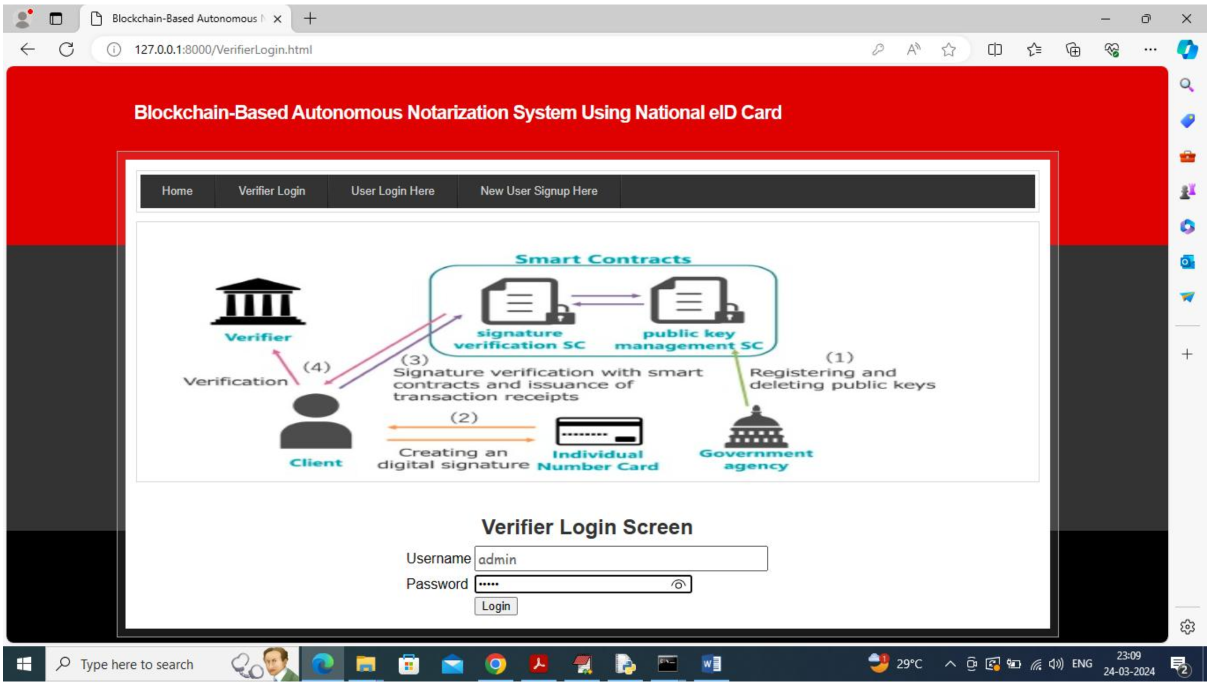
Owner Name	eID File Name	Hashcode	Signature	Date	Key	Delete Notary
kumar	second.pdf	60c586d68bda5f1de98e	1234	2024-03-24	03ac674216f3e15c761e	Click Here

Figure 5.7 : Delete Notarization
of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen user can view all notary details and can click on ‘Click Here’ link to delete notary and now logout and login as ‘Verifier’ to verify notary.

5.8 Verifier Login:

In below screen, user has to give correct pin no and eID card to verifier to verify his notary and in above screen I am giving correct details and then press Login button.


Blockchain-Based Autonomous N
127.0.0.1:8000/VerifierLogin.html
Blockchain-Based Autonomous Notarization System Using National eID Card
Home
Verifier Login
User Login Here
New User Signup Here
Smart Contracts
Verifier
signature verification SC
public key management SC
(4)
Verification
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Client
Creating an digital signature
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:09
24-03-2024

Verifier Login Screen

Username admin

Password •••••

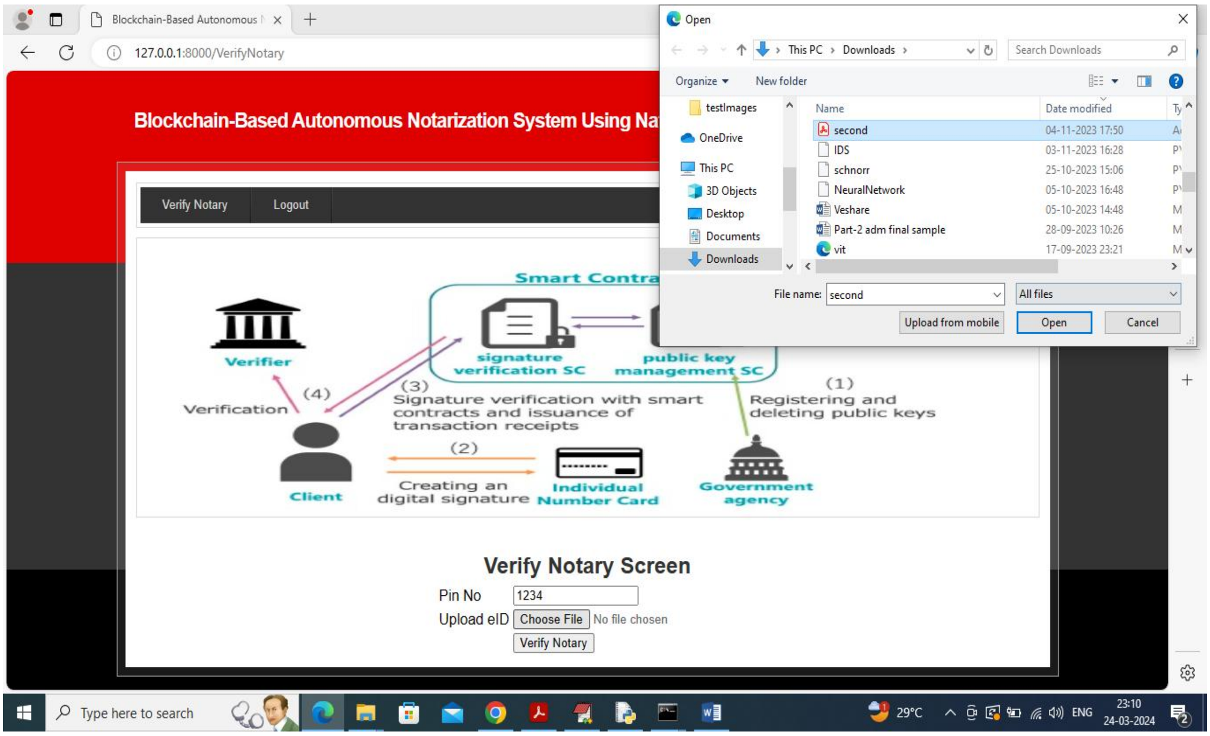
Login

Figure 5.8 : Verifier Login
of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen username and password should be given as ‘admin’, and then login we be successful as a verifier.

5.9 Verify Notary Screen :

In below screen, user has to give correct pin no and eID card to verifier to verify his notary and in above screen I am giving correct details and then press verify notary button for successful verification.



Verify Notary Screen

Pin No: 1234

Upload eID: Choose File No file chosen

Verify Notary

Name	Date modified
second	04-11-2023 17:50
IDS	03-11-2023 16:28
schnorr	25-10-2023 15:06
NeuralNetwork	05-10-2023 16:48
Veshare	05-10-2023 14:48
Part-2 adm final sample	28-09-2023 10:26
vit	17-09-2023 23:21

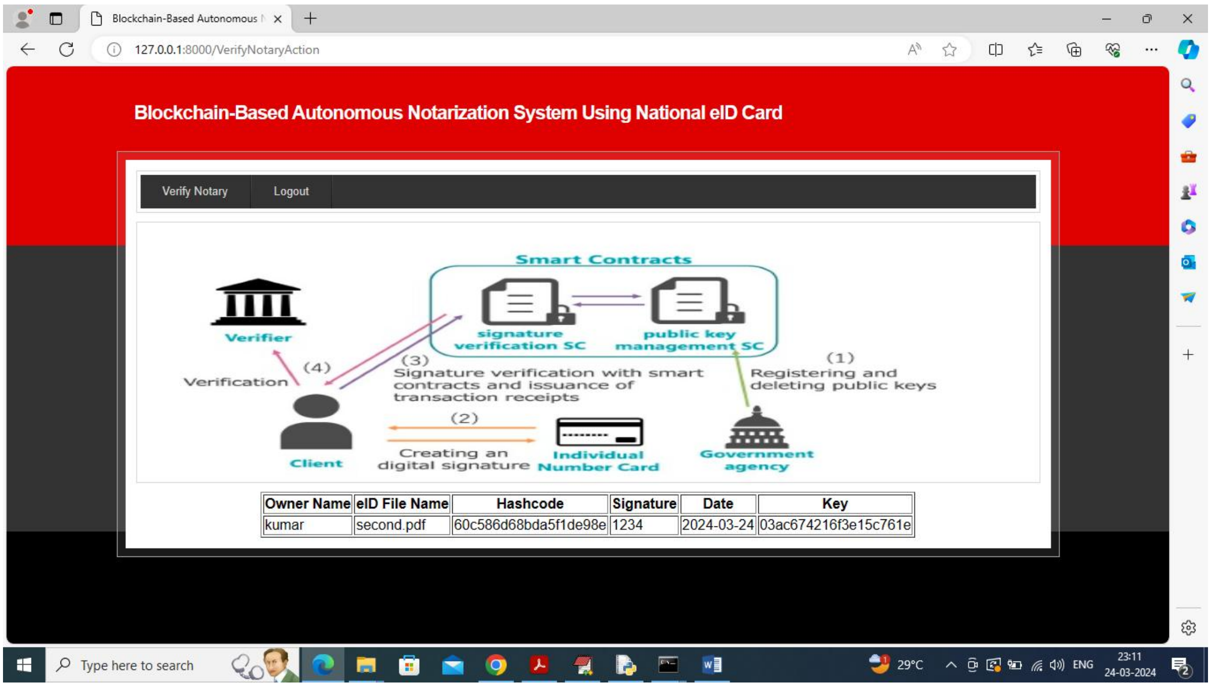
File name: second
All files

Figure 5.9 : Verifier Notary Screen of Blockchain-Based Autonomous Notarization System Using National eID Card.

In above screen if incorrect details are given i.e, entering wrong pin no and uploading wrong eID file then , we can observe that the verification is unsuccessful and we can see on the screen that verification got failed.

5.10 Verification Output:

In below screen notary is verified and 'Verifier' can view all details as proof.



Blockchain-Based Autonomous N
127.0.0.1:8000/VerifyNotaryAction
Verify Notary
Logout
Smart Contracts
signature verification SC
public key management SC
Verifier
Verification
(4)
(3)
Signature verification with smart contracts and issuance of transaction receipts
(1)
Registering and deleting public keys
(2)
Creating an digital signature
Client
Individual Number Card
Government agency
Type here to search
29°C
ENG
23:11
24-03-2024

Blockchain-Based Autonomous Notarization System Using National eID Card

Owner Name	eID File Name	Hashcode	Signature	Date	Key
kumar	second.pdf	60c586d68bda5f1de98e	1234	2024-03-24	03ac674216f3e15c761e

Figure 5.10 : "Verification output" Blockchain-Based Autonomous Notarization System Using National eID Card.

Here 'verifier' can view all the details only when entered the correct pin number and eID file.

6. VALIDATION

6.VALIDATION

The validation of the Blockchain-Based Autonomous Notarization System Using National eID Card primarily relies on cryptographic signature verification and trusted public key infrastructure (PKI) managed on a blockchain. It ensures that each notarization request is verified using the user's digital signature generated through their national eID card, cross-checked against a public key securely stored and managed by government authorities via smart contracts. This decentralized approach guarantees authenticity, integrity, and non-repudiation without human intervention.

6.1 INTRODUCTION

The validation process in the Blockchain-Based Autonomous Notarization System is a critical component that ensures the trustworthiness of each notarized transaction. It is built upon multiple layers of cryptographic and blockchain-based mechanisms. Digital Signature Verification: When a user initiates a notarization request, they use their national eID card to sign a cryptographic hash of a document. This signature is unique to both the user and the content, ensuring tamper-evidence.

The system's smart contracts utilize functions like ecrecover (in Ethereum) to reconstruct the public address from the digital signature and compare it with the one registered by the government. This process is done entirely on-chain, making it autonomous and tamper-proof. Public keys of valid users are maintained in a secure smart contract, and only authorized government agencies can register or revoke them. This ensures that only identities verified by a trusted authority can be used for notarization.

All signature verifications and notarization events are recorded on the blockchain, making them immutable and publicly auditable. This further enhances transparency and trust. The system removes the need for third-party notaries or manual verifiers by relying solely on cryptographic proofs and blockchain-based logic, minimizing human error and fraud. By leveraging these validation techniques, the system achieves high assurance in notarization, providing legal-grade, tamper-proof, and transparent digital certification of documents or agreements.

6.2 TEST CASES

TABLE 6.2.1 UPLOADING DOCUMENTS

Test case ID	Test case name	Purpose	Test Case	Output
1	User uploads Document.	To verify successful upload of a supported document	Upload a .pdf file of less than 2MB with valid metadata	Document is uploaded and hashed successfully

TABLE 6.2.2 SIGNATURE VERIFICATION RESULT

Test case ID	Test case name	Purpose	Input	Output
1	Generate Summary Valid	Validate summary after successful notarization	User-signed document, valid signature, and public key	Summary: "Signature Valid. Verified by [Verifier Name]"
2	Generate with Invalid Signature	Test handling of invalid digital signature	Manually altered signature for uploaded document	Summary: "Invalid Signature. Verification Failed."

7. CONCLUSION & FUTURE ASPECTS

7.CONCLUSION & FUTURE ASPECTS

In conclusion, the project has successfully achieved its objectives, showcasing significant progress and outcomes. The implementation and execution phases were meticulously planned and executed, leading to substantial improvements and insights. Looking ahead, the future aspects of the project hold immense potential. Future developments will focus on expanding the scope, integrating new technologies, and enhancing sustainability. These advancements will not only strengthen the existing framework but also open new avenues for growth and innovation, ensuring the project remains relevant and impactful in the long term. This strategic approach will drive continuous improvement and success.

7.1 PROJECT CONCLUSION

The Blockchain-Based Autonomous Notarization System Using National eID Card offers a transformative solution to traditional notarization by combining blockchain's transparency with the security of national identity infrastructure. Through smart contracts and public key cryptography, the system allows users to digitally sign documents using their eID cards, with signatures verified autonomously on the blockchain. This ensures that each notarized document is tied to a verifiable identity and stored in an immutable, decentralized ledger. The involvement of government authorities in managing public keys adds a trusted layer of authenticity, enabling legally sound, fraud-resistant digital notarization.

Furthermore, the system addresses key challenges in manual notarization processes such as delays, forgery risks, and high administrative overhead. By automating the verification process and providing tamper-proof records, it reduces dependency on intermediaries and increases trust in digital transactions. The use of blockchain ensures transparency and auditability, while eID integration strengthens identity assurance. Overall, this project serves as a forward-looking model for secure digital governance and has the potential to be adopted across sectors like law, finance, education, and public services.

7.2 FUTURE ASPECTS

The future aspects of the Blockchain-Based Autonomous Notarization System using National eID Card include expanding its integration with various government and private sector platforms such as land registries, legal document systems, and academic certifications. By enabling real-time, cross-platform verification of identities and signatures, the system can streamline bureaucratic processes, reduce fraud, and improve user experience in both public and private services. Additionally, adopting multi-chain or cross-chain interoperability could enhance scalability and allow integration with other national or international identity systems.

As blockchain adoption continues to grow, the system could evolve with features like biometric-based eID authentication, AI-driven fraud detection, and decentralized identity (DID) frameworks. Incorporating zero-knowledge proofs or advanced privacy-preserving technologies can also enable secure yet private verification. Overall, the project has the potential to become a foundational layer for trusted digital interactions in e-governance and beyond, supporting the shift toward a fully digital and autonomous legal ecosystem.

8.BIBLIOGRAPHY

8. BIBLIOGRAPHY

8.1 REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum Whitepaper.

[3] European Union. (2014). Regulation (EU) No 910/2014 on Electronic Identification and Trust Services (eIDAS).

[4] Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Wiley.

[5] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

[6] Koulu, R. (2016). Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement. University of Helsinki Legal Studies Research Paper.

[7] Public Key Infrastructure (PKI) Explained. (n.d.). SSL.com Knowledgebase.

[8] ISO/IEC 29115:2013. Information Technology – Security techniques – Entity Authentication Assurance Framework..

[9] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops.

[10] Estonia e-Governance Academy. (2020). eID and Blockchain: The Estonian Experience.

8.2 GITHUB LINK

https://github.com/kalyanreddy01/majorproject-blockchain-based-notarization-system