

# Cryptographically secure digital certificates on a distributed ledger

Umna Iftikhar<sup>1</sup>, Hafiz Muhammad Attaullah<sup>2,3</sup>, Inam Ullah Khan<sup>2</sup>, Muhammad Mansoor Alam<sup>2,4</sup>,  
Mazliham Mohd Su'ud<sup>2</sup>, Ahthasham Sajid<sup>2,4</sup>

<sup>1</sup>Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan

<sup>2</sup>Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

<sup>3</sup>Faculty of Computing, Mohammad Ali Jinnah University, Karachi, Pakistan

<sup>4</sup>Faculty of Computing Riphah International University, Islamabad, Pakistan

## Article Info

### Article history:

Received Jan 4, 2025

Revised Jun 13, 2025

Accepted Jul 3, 2025

### Keywords:

Certificate authority

Certificate verification

Decentralized application

Digital certificate

Smart contracts

## ABSTRACT

Verification of a qualification, achievement, quality, or aspect of a person's background is one of the biggest problems nowadays as we have seen many platforms where students can get fake credentials. Every organization must select professional and academically qualified employees to give quality service. As a result, corporations rely on academic certifications to confirm and measure their prospective employees' academic qualifications. On the other hand, these employers lack a standardized process for confirming the legitimacy of academic certificates or degrees. Because the present procedures for verifying educational certifications are time-consuming, exhausting, and costly, just a few employers verify certificates for prospective employees. This research examines the issues that are related to the smart verification of someone's credentials. To make the process of verifying digital credentials quicker, simpler, and more cost-effective, we suggest decentralized architecture. We present the prototype, design, and implementation of the proposed framework.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Mazliham Mohd Su'ud

Faculty of Computing and Informatics, Multimedia University

Cyberjaya, Selangor, Malaysia

Email: mazliham@mmu.edu.my

## 1. INTRODUCTION

Under the current situation, misleading certifications are a huge problem. Companies that recruit thousands of first-year students spend significant money to have their educational credentials and transcripts confirmed. We proposed the idea of a Digital Certification Infrastructure for the authentication of academic degrees utilizing blockchain technology to solve this challenge. The role of universities in issuing, maintaining, and certifying diplomas is costly and time-consuming. Fake academic credentials are becoming increasingly common in the country. Identifying it throughout job vetting, especially in government posts, corruption has helped the rise of this wrongdoing. Companies together with government organizations face a major struggle when it comes to fraudulent academic certificates under present-day circumstances. Companies spend substantial funds to authenticate educational diplomas because fake degree certifications have become more common. Academic credential verification processes right now involve excessive costs coupled with long delays and frequent system inefficiencies [1]. The academic institutions that issue and verify diplomas need to ensure credibility credentials while maintaining affordable management practices. A non-uniformed and non-automated verification system causes hiring of unqualified candidates who create productivity problems and weaken candidate evaluation confidence. The problem has worsened due to

improper qualification vetting alongside corruption particularly when dealing with government positions. The present situation calls for an enhanced secure and automated and cost-effective system to authenticate academic certificates and stop their improper use. Research conducted several times about blockchain technology applications relate to digital certification while focusing on maintaining data integrity [2]. The integration of blockchain technology with educational systems has become the core research objective to achieve secure academic record authentication. Research studies have suggested blockchain-based educational systems which operate decentralization while remaining publicly accessible to eliminate any power of modification or manipulation by central authorities [3]. Cryptography offers hash functions as widely adopted solutions for data integrity since they enable the validation of files and certificates without modifications to original content. Blocks of technology create unalterable yet transparent frameworks to manage certificate facilitation and validation tasks. Interface verification becomes secure through cryptographic hash functions because these tools produce specific digital certificate fingerprints [4]. Zero-knowledge proof techniques investigate methods to authenticate certificates while maintaining secrecy about sensitive information so as to improve privacy and security [5]. The development of decentralized systems has addressed multiple challenges in certificates management but scalability problems when processing numerous certificates and high costs and operational complexity as well as confusing user interfaces and privacy risks when verifying certificates persist as ongoing issues [6]. The proposed research develops an innovative blockchain system for digital certification which fixes existing system deficiencies. A different approach combines real-time verification capabilities with zero-knowledge proof mechanisms and a web-based application (CERTIFICATELY) to provide secure and convenient service. The system achieves numerous upgrades through instant certificate authentication along with free data retrieval and increases privacy through zero-knowledge proof and the capability to process large transaction loads.

Possible solutions include a database without the ability to update it, a digital signature, or a blockchain. A hash function is a function that accepts a data input and produces a predictable result output value based on that input value. When executing the hash, the output will always receive the same final work for whatever x input value. As a result, a hash function takes input (that can be any data, such as integers, and files) and produces a hash. A hexadecimal number is commonly used to represent a hash. Cryptography Hash functions. There are many uses for hash functions, but file integrity check is one of the most common. Hash functions on data files are generated with it. This application gives the user confidence in the data's accuracy. In this paper we have developed a solution that can generate a blockchain based digital certificate and it can be verifiable any organization or institute or a student itself.

- The institute can generate a digital certificate using blockchain technology.
- The student or any verifier can verify the hash of the digital certificate at any time with the web application name as CERTIFICATELY and download the digital certificate.
- Zero-knowledge proof has been employed in the design of the suggested scheme to ensure the application's.

The research proposes a blockchain-based digital certificate structure which integrates real-time authentication with zero-knowledge proof along with the CERTIFICATELY web application for providing robust security and accessibility. The platform allows certificate verification to proceed without human assistance or intermediates providing instantaneous accurate results. Zero-knowledge proof in this system ensures private data protection while enabling certificate authentication. The blockchain system enables users to retrieve stored certificates without charging fees as CERTIFICATELY operates without gas costs making the whole process more affordable and simple to use. Users can navigate the platform through a user-friendly design which lets institutions and verifiers carry out certificate documentation and verification operations efficiently. The system maintains its performance at peak levels even when handling extensive transaction activities because its design supports high scalability.

Primary contributions of this research paper consist of these key points.

- Blockchain technology uses cryptographic hashing to secure data so tampering becomes impossible after data storage occurs.
- The zero-knowledge proof systems enable the system to verify credentials without leaking any sensitive information to maintain both privacy and security.
- The CERTIFICATELY platform enables automatic real-time verification needs no human involvement for manual processes thus achieving quick results with accurate verifications.
- Users benefit from no gas fees along with reduced operational expenses through free certificate retrieval on the system platform.
- The platform maintains its high-level operational performance even when handling heavy transaction volumes because its design specifically caters to increased workload demands.
- A user-friendly arrangement exists for institutions and verifiers through CERTIFICATELY that promotes smooth operations and better use experiences.

- Blockchain constructs an unchangeable transparent system to manage certificates which improves both trust levels and accountability capabilities.
- The combination of hash comparison for verification eliminates fake academic credentials and protects educational credentials against misrepresentation and deception.
- The system enables worldwide accessibility through cross-border verification since it supports expansion of its accredited institutions database to improve international certificate recognition.
- Third-party verification occurs directly between recruiters and organizations through this system without requiring representatives from issuing institutions.
- Other professional credentials and licenses could be integrated onto the system through its extension to boost system value.

The research organized in this order: Section 1 presents fundamental information about the research subject together with the critical problem areas that need focus in this paper. Section 2 establishes the foundation of blockchain-based digital certificates with two parts describing both concepts. The research study Known as Related Work is explored in section 3 to demonstrate blockchain-based digital certificate applications with verification standards. Section 4 the experimental Setup section contains both the proposed design and framework together with the programming languages. The research discusses blockchain-based digital certificates with their verification features along with all components required to construct such a system. Section 5 details the system implementation through smart contracts creation for all modules along with presented code snippets. Section 6 describes the study of the Result and discussion. Section 7 performs an analysis of Verification scenario verification operations on Blockchain through performance evaluation while discussing its outcome in depth. Section 8 describes the brief conclusion and future implications.

#### A. The blockchain

Blockchain technology facilitates collaborative information sharing among multiple individuals, enabling them to collectively manage a database of products through a consensus mechanism. This agreement hinges on the principle of acknowledging each participant's contributions to extending the database, ensuring its integrity against tampering, unauthorized modifications, or disruption. Notably, cryptocurrencies like Bitcoin represent prominent applications of Blockchain [7]. In the realm of permissionless block-chains [8]. The chosen consensus method dictates the system's effectiveness and adaptability. Consensus systems must navigate challenges such as blockchain forks, Node domination, performance limitations, and potential consensus failures. Two prevalent methods for achieving permissionless consensus are Proof of Work (PoW) and Proof of Stake (PoS). PoW: PoW operates by prompting nodes to engage in competitive efforts to solve cryptographic puzzles, thereby constraining a node's capacity to tamper with the blockchain ledger. Successfully resolving the puzzle earns the node a reward in the form of local cryptocurrency, serving as a motivational factor [9]. Notably, PoW serves as the consensus algorithm for various blockchain systems, including Ethereum and Bitcoin [10]. In the context of an integer, the PoW function entails taking a dataset and generating both a hash value PoW and nonce values consisting of random bits, illustrating a fundamental aspect of the PoW consensus algorithm. PoS: A PoS solution addresses the issue of PoW's high energy cost. Table 1 presents a detailed comparison between PoW and PoS, two of the most widely used consensus mechanisms in blockchain technology. PoW, utilized by blockchains like Bitcoin, relies on miners solving complex mathematical problems to validate transactions and add new blocks to the chain. It delineates key characteristics, advantages, and limitations of each approach, aiding in the assessment of their suitability for various blockchain applications [11]. This process ensures security but requires significant computational power and energy, leading to concerns about sustainability. On the other hand, PoS, implemented by blockchains like Ethereum 2.0 [12], eliminates the need for intensive computation by selecting validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. This approach significantly reduces energy consumption while maintaining decentralization and security [13]. The table also compares factors such as scalability, transaction speed, hardware requirements, and susceptibility to attacks, emphasizing the trade-offs between the robustness of PoW and the efficiency of PoS in different blockchain applications. This consensus method chooses random system stakeholders to append blocks to the blockchain. The follow-Satoshi algorithm is one such implementation, in which a random native currency is chosen randomly, and the owner of that money can attach it to the blockchain and therefore collect a block reward. Users' stakes of coins contributed are reduced, and users are penalised if they offend when contributing a block to the system [14].

Permissioned blockchain consensus: only known parties can participate in the consensus to connect blocks to the block-chain on a permissioned blockchain network [15]. Because the nodes in the network are usually semi-trusted and there are fewer of them than in permissionless architecture, it allows for a higher amount of transactions per unit of time than in permissionless architecture. Different consensus mechanisms can be executed on a permission block. In such architectures, methods such as Paxos, RAFT, and various

byzantine fault tolerant (BFT) methods are known to overcome the consensus problem [16]. The Hyperledger [17] is a prominent permissioned blockchain. Figure 1 shows the concept of a blockchain that connects with multiple nodes, and each node is connected with the other while the issuer sends the transaction and the receiver receives it [18]. Its distributed ledger system securely records and links data blocks, ensuring immutability and fostering innovation across diverse industries.

Table 1. Compares technologies utilizing PoW and PoS consensus mechanisms

Blockchain technology	PoW	PoS	Description
Bitcoin	Yes	No	Transaction validation in Bitcoin depends on PoW because miners solve mathematical problems for block creation and blockchain expansion. The network security system requires high computational power in addition to large energy utilization.
Ethereum	Yes	No	The initial transaction verification method of Ethereum was PoW before developers adopted PoS with Ethereum 2.0 as both an upgrade for scalability and energy efficiency.
Binance Coin	No	Yes	Binance Smart Chain operates through the PoS consensus mechanism enabling quick and affordable deals with lower energy needs.
Polkadot	No	Yes	The Polkadot network executes transactions through its nominated PoS (NPoS) system letting validators get selected by nominators thus improving system decentralization as well as operational speed.
Uniswap Bitcoin Cash	No	Yes	Uniswap functions as a decentralized exchange (DEX) developed for operation on the Ethereum blockchain. The Ethereum network transition to PoS power the use of PoS through an indirect connection.
Bitcoin Cash	Yes	No	Bitcoin Cash functions as a Bitcoin fork which maintains PoW protocols to verify network transactions at the expense of faster and cheaper procedures compared to Bitcoin.

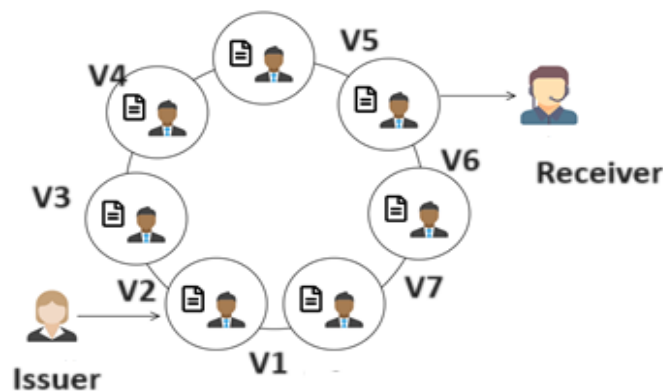


Figure 1. Blockchain, the cornerstone of decentralization, epitomizes trust and transparency in digital transactions

Transactions in merely this public blockchain are now almost instantaneous because it relays the nodes inside the system and maintains identifiers for each node. To execute consensus in the network, it supports multiple consensus mechanisms including practical byzantium fault tolerance (PBFT), Sifter, and cross-fault tolerance (XFT). Table 2 provides a detailed comparison of the requirements and characteristics of permissionless blockchains, permissioned blockchains, and traditional databases, focusing on their structure, access control, and operational needs. This visual comparison highlights the resilience and reliability of blockchain technology in maintaining data accessibility compared to conventional database systems. Permissionless blockchains, such as Bitcoin or Ethereum, operate in a decentralized manner and are accessible to anyone without restrictions, relying on consensus mechanisms like proof-of-work or proof-of-stake to validate transactions. In contrast, permissioned blockchains are semi-decentralized, granting access only to authorized participants and typically employing lighter consensus mechanisms, such as Byzantine Fault Tolerance, for higher efficiency. Traditional databases differ significantly, as they are centralized systems managed by a trusted authority [19], allowing only designated users to perform operations. The table also explores aspects like scalability, data integrity, security, and energy efficiency, highlighting how these systems cater to different application scenarios, from public networks to private enterprise solutions. It performs best when there are a few devices in the cluster, and it cannot be expanded effectively if any are added [20].

Table 2. Illustrates the comparative availability performance between blockchain and traditional databases, with ✓ symbolizing high availability, ● representing average availability, and× indicating unavailability

Characteristics	Requirements	Permissionless	Permissioned	Database
Confidential	There aren't enough trusted third parties. Immutability	✓	✓	×
	and Accountability Several untrustworthy authors	✓	✓	✓
	Transactions between individuals are known as peer-to-peer transactions.	✓	✓	●
		✓	✓	×
Interpretation	Transactional traceability Transaction verifiability	✓	✓	×
	Notarization of data/transactions in context Data security	✓	✓	×
	Transparency Disclaimer	✓	✓	×
		✓	×	×
Reliability	Transaction	×	●	✓
	Speed and latency	✓	✓	×
	Costs of upkeep	✓	✓	●
	Fragmentation Extensibility	×	●	✓
Consensus Algorithm	Engagement guidelines. Verifiers are required.	✓	✓	●
	Autonomous/dynamic interactions between distinct writers' transactions.	✓	✓	×
		×	×	×

Permissioned blockchain consensus: digital certificates are a type of electronic identity used by any peer who wants to communicate securely with another peer over the internet. In asymmetric situations, digital certificates are employed. Cryptography which would be a type of cryptography that uses crucial pairs. The duo comprises a public and a private entity. A public key, which anybody may access, and a personal address, which the owner keeps private. Any of those keys can be used to encrypt or decrypt data, so anything encrypted with them can be decoded. Only one key can de-encrypt the other, and vice versa. Moreover, one of the essential information in certificates is the peer's public key, which allows communication. I partner to communicate their digital certificates in a verified manner [21]. These certificates include assurance from a trusted source that the certificate's secret key belongs to the certification's subject. In all other words, the party is who it claims to be. The name of this trusted source is a certificate authority (CA), which will be described later [22]. The storage of achievement and recognition records, such as degree certificates, is a self-evident educational function. The grant-ing institution would save the certificate information in the blockchain, which the under study may access, share with bosses, or access through a web. It keeps a constant open record, protected from modifications to the organization or the loss of its private documents. This creates opportunities for trusted professionals and instructors to give certificates and identifications in a coordinated manner. The blockchain gives transparent proof that a regulating personality funded an understudy personality, but it does not confirm either party's trustworthiness in and of itself. The blockchain can quickly and reliably validate the existence of an activity, such as the issuance of a certificate, but not its legitimacy.

Blockchain based certificate: digital certificates are a type of electronic identity used by any peer who wants to communicate securely with another peer over the internet. In asymmetric situations, digital certificates are employed. Cryptography which would be a type of cryptography that uses crucial pairs. The duo comprises a public and a private entity. A public key, which anybody may access, and a personal address, which the owner keeps private. Any of those keys can be used to encrypt or decrypt data, so anything encrypted with them can be decoded. Only one key can decrypt the other, and vice versa. Moreover, one of the essential information in certificates is the peer's public key, which allows communication. I partners to communicate their digital certificates in a verified manner. These certificates in-clude assurance from a trusted source that the certificate's secret key belongs to the certifi-cation's subject. In all other words, the party is who it claims to be. The name of this trusted source is a CA, which will be described later [23]. The storage of achievement and recognition records, such as degree certificates, is a self-evident edu-cational function. The granting institution would save the certificate information in the blockchain, which the understudy may access, share with bosses, or access through a web. It keeps a constant open record, protected from modifications to the organization or the loss of its private documents. This creates opportunities for trusted professionals and instructors to give certificates and identifications in a coordinated manner. The blockchain gives transparent proof that a regulating personality funded an understudy personality, but it does not confirm either party's trustworthiness in and of itself. The blockchain can quickly and reliably validate the existence of an activity, such as the issuance of a certifi-cate, but not its legitimacy.

Verification of smart contracts: blockchain technology enables a distributed computing system in which the participants concur on a single history of transactions, making the transactions public. After be-ing divided into blocks and given timestamps, the transactions are published. Each block's hash builds on the

previous block's hash to create a chain, making it challenging to change published blocks. The use of blockchain technology is how computer systems can control how real-world parties interact with one another in many different ways. The prerequisites for the involvement of reliable central authorities or the usage of resource managers restricted the adoption of smart contracts on the blockchain. Specific Blockchain systems' implicit enforcement of smart contracts has created wealth of new possibilities [24].

Deployment of smart contract: the verified contracts can be implemented on the platform on top of blockchains. Those who store contracts on blockchains cannot. Because blockchains are immutable, they cannot be changed. A new contract must be written for each amendment. The contracts are accessible to all parties via the Blockchains after the implementation of smart contracts. Additionally, both parties are involved. The smart contract locks the parties by freezing the equivalent digital wallets. For illustration, the coin on the wallets, transfers can be made inward and outbound. Blocking words that pertain to the contract. However, the Parties' digital wallets can be used to identify them [25]. In Figure 2 through a suitable web browser or the built-in browser of the mobile app, MetaMask enables users to safely connect to decentralised applications, save and keep account keys, broadcast transactions, transmit and receive Ethereum-based money and tokens, and broadcast transactions. It showcases the sequential stages from coding and compiling to uploading and execution, elucidating the intricate steps involved in implementing self-executing agreements on a decentralized network.

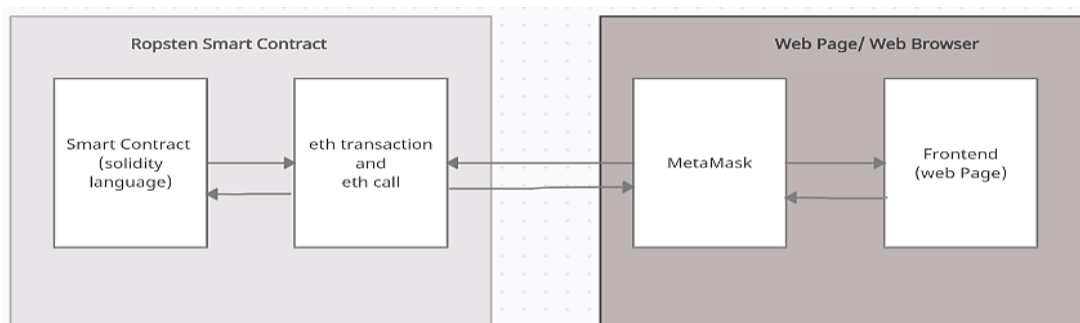


Figure 2. Deployment process for a smart contract, a pivotal aspect of blockchain technology

Zero-knowledge proof: a zero-knowledge statement protocol in cryptography is how one person (proof of claim) can verify the other entity (validator) that the specific information is accurate. At the same time, the one that proves does not transfer every additional data other than the fact that the data is correct. The premise of zero-knowledge arguments is straightforward to demonstrate knowledge of some information simply by disclosing the situation. Verifying such information without releasing the truth or additional data is the problem [26]. The zero-knowledge proof system is a crucial area of computational complexity theory and cryptography that has attracted a lot of attention since it was first presented. A single communication from the prover to the verifier is all that is contained in a non-immersive zero-knowledge proof system. It is frequently employed in creating numerous crypto-graphic protocols and algorithms due to its strong authentication, decent privacy, and low interactive complexity [27].

Hash function: a hash function can be defined as taking an input value and generating a predictable output value based on that input value. When executing the hash, the output will always receive the same Y final output for whatever X input value [28]. Each input has a pre determined output in this manner. Depicts the situation, as a result, a hash function takes in-put and produces a hash. A hexadecimal number is commonly used to represent a hash [18]. There are other hashes algorithms, such as (MD, and SHA), which are the most widely used hash functions. Hash functions are usually irreversible (one-way), which implies that if you only know the output, you won't be able to find out the input unless you test every possible input [29]. Figure 3 illustrates a cryptographic protocol that enables secure verification of information authenticity without exposing sensitive details to the verifier. Through a series of interactions, the prover convinces the verifier of a statement's truth-fulness, showcasing the power of privacy preserving techniques in secure data transactions. In this process, the prover demonstrates to the verifier that a statement or data is valid, while withholding the specific details of the information being verified [30]. By ensuring that sensitive data remains undisclosed, this protocol facilitates secure interactions, enhances trust, and upholds data privacy in various digital environments. There are several uses for hashing functions, but file integrity check is one of the most common. Hash functions on data files are generated with it. This application gives the user confidence in the data's accuracy [31].



Figure 3. A cryptographic protocol enabling one party to verify the authenticity of information without revealing any sensitive data to the verifying party

## 2. TECHNICAL HISTORY

The certification of competencies and academic credentials plays a principal part in modern societies and ways of life. Classically, such a certification is performed through paper certificates containing seals and marks. These documents, however, have no consistency among distinctive nations and no recognized computerized proportionate and, most vitally, are subject to distortion. A few cases confirm this happened in recent years, as within the case of the dignity of confirmations at the massachusetts established of innovation (MIT), who announced to have manufactured and lied almost her instructive qualifications for 28 a long time [32]. In this setting, a universally recognized standard for digitizing and verifying competence certificates (as transcripts, and recognitions) and scholastic qualifications is a must. Besides providing solid confirmation instruments, such a framework should also set up a globally recognized arrangement for transportability and verification of competencies. Open Badge [33]. The scope of Open Badge is to provide organizations and teachers with a system for issuing advanced identifications to the competent owners to recognize not as if it were their official learning but indeed transversal aptitudes. For this reason, certificates compliant with Open Identifications are planned to provide a point-by-point profile of the beneficiary, including the so-called Diploma Supplement [34].

The European Data Science Academy (EDSA) [35] may be an excellent example of blockchain innovation being used to provide information science skills to job seekers. EDSA, too, makes a difference by providing training to world-leading information scientists in the modern day. Information is being produced at an incredible rate from all enterprises in the twenty-first century, posing several issues regarding data collection, capacity, and analysis. However, as the amount of information available grows, so does the demand for professionals with the necessary skills to supervise and govern it. As a result of this requirement, the EDSA was established to provide a platform for monitoring the producers and consumers of information systems specialists by providing real-time expertise preparation.

Learner-Centered Blockchain of Open University in U.K. The Open University of the United Kingdom [36] Using blockchain technology, a learnercentred approach to learning has been spread. They demonstrated a beginner environment using blockchain in that paper. The student, instructor, courses, teaching fabric, validation system, and learner's association are all included in this biological system. The students are enrolled in various courses and access additional learning resources. Mentors and other instructional personnel provide informal and formal advice as part of the learner's entire summit and developmental evaluation. Central regulatory organizations give official certifications indicating that their institutional processes have been agreed upon. Each learner has an identity and achievement visualization area called a visa, which may be utilized instead of a traditional resume to show the boss his or her abilities. Transparency, trust, safety, and security are all provided by this architecture.

In U.C. Davis's Computerized Identification System, these fundamental competencies are presented as a 'digital badge' [37], there are five levels to each competency: aptitude, information, honor, involvement, and competence. The 'digital badge' framework is a human capital assessment methodology that validates the core competencies within the portable connected society are easy and straightforward.

Microsoft Exam and Certification Badge Microsoft teamed up with Pearson VUE's Recognition stage to provide a unique identifier for certification purchases. A Microsoft certification stamp, available on the internet and containing photos and unique metadata about the certificate holder, could be used as identification. The identification provides the owner with complete information about the innovation and establishes ownership [38]. Table 3 provides a comprehensive comparison of existing studies on blockchain-



based digital certificates, highlighting key aspects such as security, scalability, efficiency, and application scope. It examines the methodologies employed, the types of blockchain used (e.g., public, private, or consortium), and the mechanisms for certificate issuance, storage, and verification [39]. The table also contrasts the integration of cryptographic techniques, such as hashing and digital signatures, to ensure data integrity and authenticity [40]. Interventionary studies involving animals or humans, and other studies that require ethical approval, must list the authority that provided approval and the corresponding ethical approval code.

Table 3. Presents a comparative analysis of related works focusing on blockchain-based digital certificates

Blockchain based digital certificates	Methodology	Limitations
Decentralized Attestation of Conceptual Models Using the Ethereum Blockchain [13]	The availability of cryptographic certificate documents that publicly certify that mentioned immutability and transparency in the paper	Difference in the blockchain network
A Preliminary Review of Blockchain-Based Solutions in Higher Education [27]	According to a preliminary examination and study of these cases, this research shows a studentcentred approach and several critical use cases in the educational arena	It was restricted since that established only a permissioned blockchain public entire network.
Application of Blockchain Technology in Higher Education [28].	The authors also published a realworld case study after verifying the MIT certification	This study investigates how blockchain technology affects the sector of education.
Blockchain-Based Framework for Educational Certificates Verification [29]	Fordegree verification, that developed a blockchain hyperledger fabric framework.	No endorsers or ordering management in the desktop application
Blockchain Ecosystem for Verifiable Qualifications [30]	The answer to higher education linked institutions to register the issuance of degrees via Check the blockchain, including the certificate trustworthiness	No endorsers or ordering management in the desktop application
Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology [31]	This proposed approach offers a remedy for Indonesia's postsecondary education system. The fundamental goal is to provide high-quality education throughout the country.	Limited to a particular location, collaborative artificial intelligence platform.

The proposed decentralized framework offers a solution to these longstanding challenges by leveraging blockchain technology, allowing for a transparent, immutable, and streamlined process that can be accessed and utilized across different organizations and sectors. By shifting from a model dependent on individual trust to a network-based validation, this research aims to foster a universal standard for verification [41]. The decentralization of the verification process not only reduces the time and financial costs involved but also enhances the reliability and integrity of academic and professional credentials. In highlighting these motivations and identifying the shortcomings of existing practices, this research contributes a valuable perspective and a practical solution to a problem of growing relevance in today's increasingly digital and globalized workforce. Figure 4 provides an insightful representation of the architectural diagram of the proposed system, which has been meticulously designed to address certain inefficiencies and shortcomings observed in previous studies. The motivation for developing this new architecture emerges from a profound need to enhance specific functionalities and performance criteria that were either inadequately addressed or completely neglected in existing models [42]. The architecture illustrates a novel arrangement of components, interactions, and workflows that aims to offer a more streamlined, robust, and scalable solution. One of the key gaps identified in previous studies was the lack of integration between disparate subsystems, leading to bottlenecks and hindrances in the data flow [43]. The proposed architecture emphasizes seamless interconnectivity and a harmonized approach that fosters efficiency and adaptability. Furthermore, the incorporation of innovative technologies and methodologies signifies a progressive shift towards meeting the demands of contemporary applications. This architectural evolution not only offers practical advantages but also symbolizes a conceptual advancement, aligning more closely with current industry standards and expectations. By addressing these gaps, the new design delineates a path toward a more coherent, resilient, and future-ready system, making it a significant contribution to the field.

### 3. PROPOSED FRAMEWORK

The proposed blockchain-based system named Certificately, which revolutionizes digital certificate authentication and verification processes. This innovative web application utilizes zero-knowledge proof to ensure the validity of contracts while preserving user privacy by withholding unnecessary information. By leveraging the inherent security of blockchain technology, Certificately effectively combats issues



surrounding fraudulent and unverifiable certifications. Certficateely operates by verifying contract authenticity through unique account addresses and transaction hashes, securely embedded within the immu-table structure of the blockchain. This approach guarantees the integrity and tamper-proof nature of certified documents. The system caters to two primary user groups: students and organizations or enterprises. For students, Certficateely offers a platform to present credible and easily verifiable certificates, enhancing their credibility and trustworthiness in the eyes of potential employers or academic institutions. On the other hand, organizations and enterprises benefit from the streamlined verification process, eliminating the need for time-consuming manual checks and reducing administrative overheads.

By addressing the privacy concerns of individuals and the efficiency requirements of institutions, Certficateely provides a comprehensive solution to the challenges associated with fraudulent certifications. In an era where the prevalence of counterfeit credentials poses a significant threat, Certficateely stands as a robust and trustworthy system, merging the transparency and security of blockchain technology with the practical needs of mod-ern education and business environments.

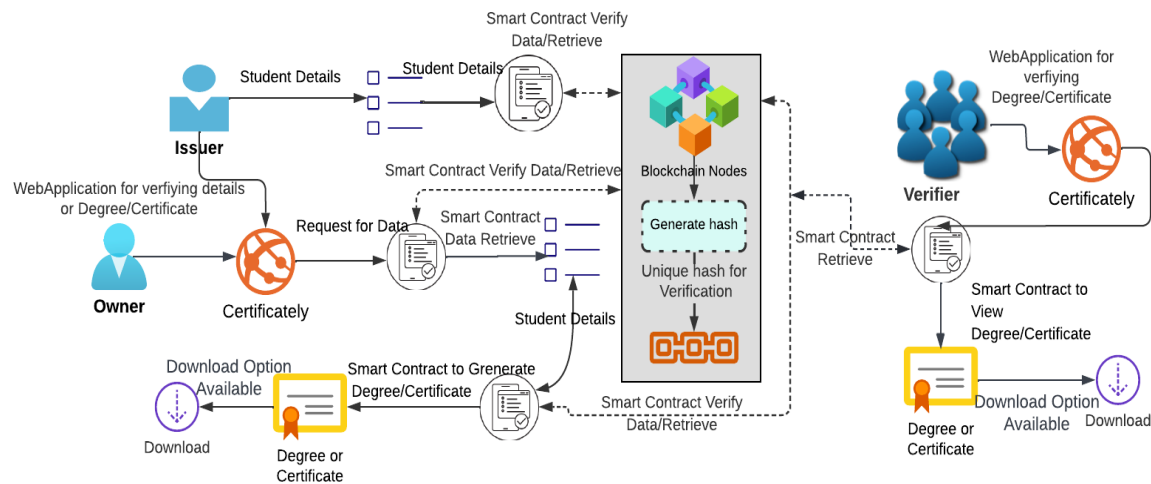


Figure 4. Architectural diagram of the proposed system

### 3.1. Components of proposed framework

The proposed system consists of several key components aimed at managing data exchange within a blockchain-based network, ensuring secure transactions and maintaining data integrity and security. At the heart of this system is a brows-er-based program called the Certficateely web application, tailored to meet these spe-cific requirements. Through dedicated web pages, Certficateely confirms adherence to predefined protocols and standards, thereby enhancing trust and transparency in transactions. The integration of blockchain technology adds an additional layer of trust and transparency to the system. Every transaction within the network is rec-orded and can be verified, by leveraging cryptography and distributed ledger technology, the system fosters an environment conducive to accountability, making it applicable across various sectors, including finance and healthcare. With-in the system, roles such as Issuer and Owner play crucial roles in managing creden-tials and ensuring their authenticity.

- Issuer: The Issuer, typically the root entity in the system, can grant sub-issuer access to other nodes, thereby delegating certain credential management tasks. This permis-sion-based sub-issuer registration ensures controlled access and prevents unauthorized entities from assuming sub-issuer roles.
- Owner: on the other hand, are holders of credentials issued within the system. When a holder requests to use a credential, the issuing organization's entry in the holder's creden-tial account is transferred or created, depending on the scenario. Sub-issuers play a role in creating and managing Credential Proof resources, which are essential for verifying cre-dential authenticity.
- Verify: Verification processes within the system involve matching hashes and holder ad-dresses, followed by authentication using time stamps and signatures. The system aggre-gates basic credentials and verifies their authenticity through verification of the associated digest. Testing for digest in the credentials account ensures that revoked resources are no longer accessible, maintaining the integrity of the verification process.

### 3.2. Experimental setup

The blockchain-based certification system outlines all functions and tasks between its four main components which include admin, student, issuer and verifier. The system functions through the Admin's account management duties while Students start credential requests and maintain control over them and Issuers decide credential issuance and verification and Verifiers check the validity of received credentials. The research experiments use a detailed description of the blockchain selection process such as Ethereum or permissioned systems along with PoW or PoS consensus and block capacity and speed measurements. The document presents the development tools alongside the frameworks for building smart contracts and issuing certificates as well as validating credentials and describes the visible components of the interface. Detailed documentation allows researchers to recreate the system's implementation and performance evaluation which increases both reliability and credibility of the proposed solution. The admin role assumes the central authority position, responsible for overseeing system settings and user management, ensuring strict adherence to designated protocols and standards. The student role engages directly with the system, initiating credential requests, managing personal information, and interacting with issuers and verifiers as necessary. The Issuer role, commonly associated with educational institutions or certification bodies, holds the responsibility of granting credentials, verifying achievements, and safeguarding the integrity and authenticity of provided information.

Lastly, the Verifier role, represented by entities such as employers or universities, validates credential validity by cross-referencing student-provided information with data from original authorities. In Table 4 The experimental setup for the blockchain-based digital certificate involves a detailed description of the various parameters, configurations, and tools used to evaluate the system's performance. This includes the selection of the blockchain platform, such as Ethereum or a permissioned blockchain, and the specific network configurations, including the consensus mechanism (e.g., PoW or PoS), block size, and transaction processing speed. The setup also defines the tools and frameworks employed for smart contract development, certificate issuance, and validation, as well as the user interface for interacting with the system.

The barrier system operated through a combination of Windows 11 together with React (19.0.0) for front-end tasks, Node.js (20.0.0) for server responsibilities along with dependency management through NPM (8.0.0). The system adopted Bootstrap version 6.0.0 for responsive design while Express.js version 5.0.0 managed API development and server routing features. The system used ES2025 JavaScript along with HTML5 and CSS3 to implement business logic functions. The implementation of Solidity version 0.9.0 created smart contracts while Web3.js version 2.0.0 enabled blockchain communication. Student records and credential data were handled by a MySQL (9.0) database layer which provided both data security and integrity features. The configuration provides an expansion-ready platform which delivers safe digital certificates and performs operations effectively.

Table 4. Presents a comparative analysis of related works focusing on blockchain-based digital certificates

Methodology	Description
Operating system	Windows 11 is used for the application level, which builds and administers the web application and database layers.
Framework	<b>React</b> that used version 16.13.0 for the front-end of the application layer. <b>Node</b> version 14.15.0 used for the integration with web Application. <b>NPM</b> version 6.14.8 used to install the necessary libraries and provide the middleware's running functionality. Bootstrap v5.1 for designing web Applications. <b>Node.js19</b> – A Javascript-based platform for constructing high-performance, scalable online applications. <b>Express.js20</b> – Express.js is a Node.js framework that provides route abstractions, middlewares, and other features to make creating application programming interfaces easier (API).
Languages	<b>HTML</b> Front-end Designing language used on the application layer. <b>CSS</b> Front-end styling language used on the application layer. <b>JavaScript</b> is used for the business logic of the whole application layer and middleware. Solidity is the language for writing the smart contract for the blockchain. <b>Web3Js</b> for connectivity between the browser and the application.
Database	<b>MySQL</b> - An open-sourced database enables database deployment inside a machine for the control service to keep records of all registered students and other important information. The structured database will be detailed in the Database section.

### 3.3. Registration module

When a new registration for a certificate is added, this procedure is triggered. After that, the Certificately App will process the certificate and send a transaction to the Ethereum blockchain network. The certificate's hashes and details are recorded using the smart contract's addDetail(). When the relevant transactions are already included in a newer Ethereum block, it is recorded as an addition to the blockchain. The Etherscan Blockchain Explorer website can provide you with this information.

### 3.4. User details module

When a holder signs up with an issuance, they can request a credential account resource, which can use to store credential proofs resulting from meeting the issuer's requirements on the way to getting credentials from them. Conceptual diagram of student of certificate. When a holder registers with an issuing, they can seek a credential account processes supply, which could hold credential proofs obtained by completing the issuer's requirements on the path to receiving credentials.

### 3.5. Add details module

Able to register with an issuer" refers to the procedure of the issuer transferring faith in government to the holder. Whenever a central issuer registers a holding in the implementation, an empty record in credential account is created for the holder. If the owner claims the credentials, the issuing institution's credentials account item is transferred to the owner's credential accounts if one currently exists, or a new professional certification account is established if one does not. A sub issuer produces an empty Credentials Proof property and stores it in the Log Proofs resource when it registers a holder.

### 3.6. Verification module

When a holder signs up with an issuance, they can request a credential account resource, which can be used to store credential proofs resulting from meeting the issuer's requirements on the way to getting credentials from them. Conceptual diagram of student of certificate. When a holder registers with an issuing, they can seek a credential account processes supply, which could be used to hold credential proofs obtained by completing the issuer's requirements on the path to receiving credentials. Conceptual diagram of certificate student.

### 3.7. Generate certificate

The blockchain certificates smart contract functions as a transparent and immutable ledger for certificate-related data. When a holder signs up with an issuance, they can request a Credential Account resource, which can use to store credential proofs resulting from meeting the issuer's requirements on the way to getting credentials from them. Conceptual diagram of Student of Certificate. When a holder registers with an issuing, they can seek a Credential Account processes supply, which could hold credential proofs obtained by completing the issuer's requirements on the path to receiving credentials. It exemplifies how blockchain technology is not just revolutionizing financial transactions but also has broad applications in areas like education and credential verification, offering transparency, security, and efficiency.

### 3.8. Verify certificate module

Students or verifiers can see the certificate and verify the Hash at any time. View Certificates shows a list of all the available certifications in a single account. To obtain and display all certificates, it scans each generated Certificate contract from the blockchain using the Transaction. After entering the student's address and Hash, the result will return the student's complete details, including Hash. In Figure 5 Conceptual diagram of Student of Certificate resource.

The account is validated using the browsers plugin Metamask for authenticating a user on the web app with their associated account, enabling the servers to know whose account is registered on the blockchain and it facilitates understanding of the verifier's role and responsibilities in the authentication process. The authenticated account through Metamask is required for operations with the student's certificates display manipulation and Educational Organization's certification management.

Transaction costs in blockchain technology are made up of various layers of fees gathered by financial institutions. Financial transactions involving financial intermediaries take a long time and require a lot of resources, including time and money. Blockchain technology, on the other hand, speeds up the transmission of financial operations, reduces their cost, and does away with the need for financial institutions.

### 3.9. Download certificate module

This module is designed to provide a seamless and secure experience for users to access their certificates. The process begins with the user logging into the system through a secure authentication mechanism. Once authenticated, the user navigates to the certificate retrieval section, where they can view a list of available certificates linked to their account. The interface typically provides options to preview certificate details, ensuring users select the correct document. A system that transforms facts about users' educational experience into a form of digital assets is called a permanent global record of intellectual exertion and accompanying reputation reward. Figure 6 illustrates the "Download Certificate" module, detailing the user interface and workflow for retrieving digital certificates from a blockchain-based system. Upon confirming their choice, the system interacts with the blockchain network to verify the certificate's authenticity and integrity.

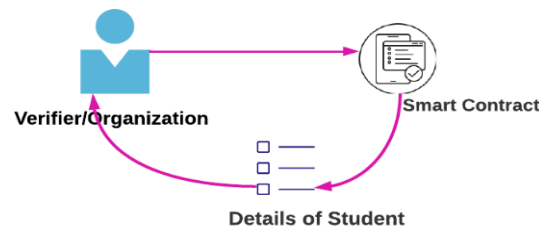


Figure 5. The access permissions granted to verifiers within the system, specifying the actions they can perform and the data they can access

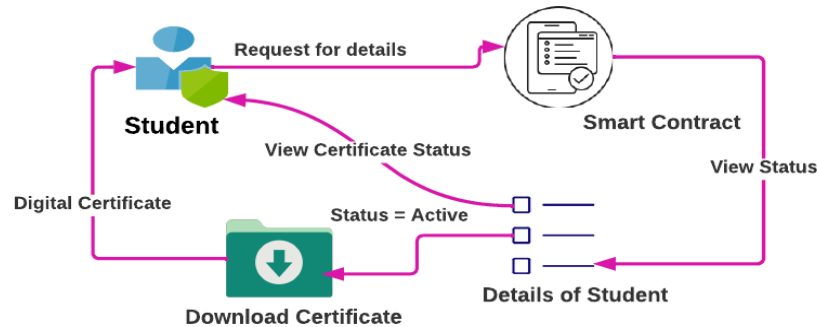


Figure 6. The 'Download Certificate' module, showcasing the user interface and workflow for retrieving digital certificates from the blockchain-based system

#### 4. ALGORITHMS

The following algorithms are used to elaborate the how to set certificate 1, how to verify certificate 2 and how to view details of a student. The Algorithm 1 shows how students can store their information in the blockchain. The Algorithm 2 shows how anyone can publicly verify their credentials or details with a created website that retrieves all the information from the blockchain. The Algorithm 3 shows how a verifier or any student can view details.

##### Algorithm 1. Set Certificate Algorithm

```
Require: UsersAttr,
Return, True or False
1: MainAttribute ← this.details();
2: SearchMainAttribute ← this.getAttribute(MainAttribute);
3: CertificateContract ← AttrContract.getdetails(Attr)
4: if CertificateContract.DetailsContract(Attr) = true then
5: If CertificateContract.DetailsContract(MainAttribute, UsersAttr) = true
6: GetPermissionToAccess
7: else
8: Return False
9: end if
```

##### Algorithm 2. Verification of Certificate

```
Require: UsersAttr,
Return, True or False
MainAttribute ← this.certificate()
OtherAttribute ← this.status();
If student.status == approved
If student.hash == verified
Display.Certificate();
```

##### Algorithm 3. View Details Algorithm

```
Require: UsersAttr,
return, True or False
if msg.sender == owner then returndetails();
else
Revert()
end if
```

#### 4.1. Process flow of generate certificate

In Figure 7, when a holder signs up with an issuance, they can request a Credential Account resource, which can be used to store credential proofs resulting from meeting the issuer's requirements on the way to getting credentials from them.

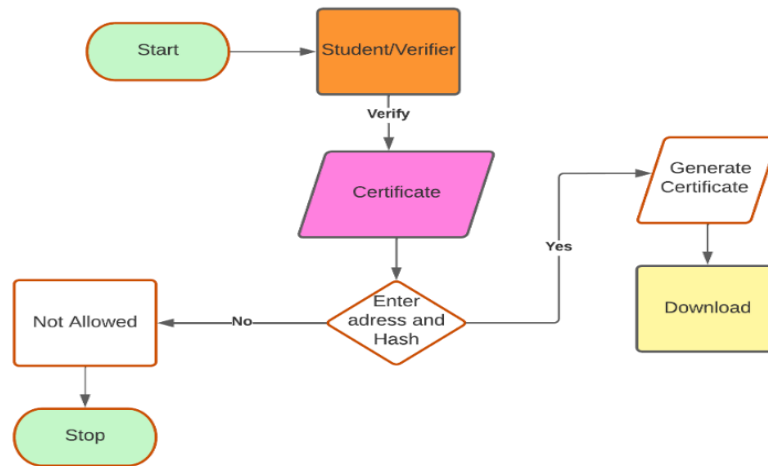


Figure 7. The flowchart depicts the 'Generate Certificate' process, outlining the sequential steps involved in creating digital certificates within the system

#### 4.2. Process flow of verify certificate

In Figure 8 Students or verifiers can see the certificate and verify the hash any time. View Certificates shows a list of all the certificates available in a single account. To obtain and display all certificates; it scans each generated Certificate contract from the blockchain with the use of the transaction. If the owner claims the credentials, the issuing institution's credential accounts entry is transferred to the holder's credentialing account if one still exists, or a new professional certification account with the latest iteration for the holder is established if one does not exist. A sub-issuer produces a new Credential Proof resource and stores it in the Log Proofs resource when they register a holder.

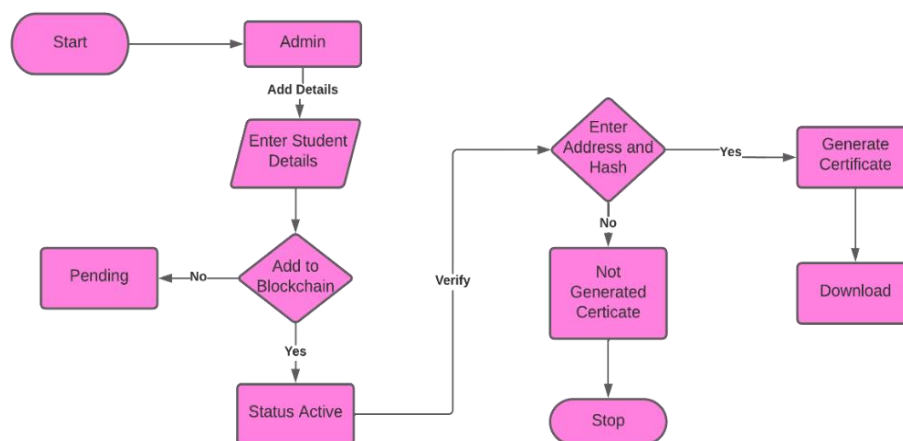


Figure 8. The flowchart illustrates the 'Verify Certificate' process, delineating the systematic steps for authenticating digital certificates within the system

### 5. IMPLEMENTATION OF PROPOSED FRAMEWORK

For both educational institutions and employers the academic certificate management and verification process has remained slow and difficult to work with. The legacy process of manual verification uses methods that struggle with both time constraints and resident human mistakes and fraudulent activities. Recruiters face significant challenges because of increased counterfeit certificate production that makes

authentic academic qualification verification impossible thus causing hiring problems together with productivity decreases. We developed CERTIFICATELY as a blockchain-powered digital certification platform which would simplify and protect every step of certificate generation and verification. The Solidity-developed smart contracts which build CERTIFICATELY automate important functions including student registration while also managing certificate generation and record authentication through cryptographic hash functions. The system presents users with intuitive web access for students and educational institutions and recruiters to instantly examine and confirm diplomas. The platform maintains a dual security system through hash-based verification because this technical component protects both data staying legitimate and prevents modifications to student records. The authentication system using MetaMask works to both increase data protection because it verifies authorized access while also protecting the modifications made to stored information. According to CERTIFICATELY users can designate personnel with assistant admin privileges to manage student records as well as update certificate statuses with maximum efficiency. Through this innovative solution organizations eliminate both administrative expenses and intermediate agencies therefore delivering prompt and secure services for verifying certificates at cost-effective prices. Through blockchain-enabled operations CERTIFICATELY enhances academic trust while guaranteeing transparency regarding academic certificates and creates a forward-thinking solution suitable for educational organizations and hiring institutions.

### 5.1. Development of smart contracts

This initiative is represented by different Smart Contracts established to manage all of the essential information, including certification and registration of students, view details of students, generating Hash, and verification of Hash management.

### 5.2. Features of web application

The web application that has been created, namely CERTIFICATELY, to view or verify details of the students as well as used for the verification of certificate moreover, there is a download option available to save or keep a record. The smart contract design and functionality for managing student information with Solidity appears in Figure 9. Figure 9(a) presents the smart contract base architecture that utilizes Student struct to arrange vital student information elements including name, academic pursuit, academic record and educational institution data. Figure 9(b) demonstrates the smart contract system which provides full-record visibility bringing enhanced clarity to stored information operation flows. Hash verification implemented in Figure 9(c) protects the contract from unauthorized changes to preserve both data authenticity and the integrity of the contract for users.

### 5.3. Features of assistant admin rights

Following are the features of assistant admin rights. The assistant admin has the right to add student details, view student details, or update status.

- Registered student the routine examines each block and associated data using PHP code to extract Certificate details starting state and confirm that the transaction's agreement is a Certificate consensus protocol. Figure 10 describes the registration process for the student.

### 5.4. Role of admin panel

Following are the roles of the admin panel. The admin has the right to view student details, or update status, generate certificate, verification of account hash, view details, verify certificate, and download certificate.

- View student details or update status the Ethereum blockchain lacks a default algorithm for searching all transactions in a single account, limiting the blockchain network's ability to access all of an account's transactions. As a result, the update routine's goal is to insert and update data into the prototype's database depending on the information inside the blockchain, keeping the database tables updated and ordered every time the update routine runs. Figure 11 describes the updating and view record process of the student.
- Generate certificate the parameters retrieved from the blockchain certificates smart contract are used to determine the certificates shown on the web page, which are displayed as: Figure 12 describes the details of the student in the certificate, and it also has a feature download button so the student and verifier can easily download the certificate.
- Verification of the account hash the account is validated using the browsers plugin Meta mask for authenticating a user on the web app with their associated account, enabling the servers to know whose account is registered on the blockchain.

The established account through Meta mask is required for operations with the student's certificates display manipulation and Educational Organization's certification management. In Blockchain technology, transaction costs consist of multiple layers of fees collected by financial organizations. Financial operations that go through financial intermediaries take a long time to complete and require a lot of resources, including time and money. Figure 9(a) A structured view of the smart contract showing how student information is recorded, Figure 9(b) the ability for users to access all stored details within the contract, and Figure 9(c) hash-based verification that ensures data integrity, secures transactions, and prevents tampering. Blockchain technology, however, speeds up this process and reduces the cost of financial transactions. Additionally, it does away with the need for financial institutions.

```

1 function Adddetails(address a, string memory sname , string memory scourse,
2 string memory atte,string memory inst , string memory _cid, string memory dt, string memory _Sta ,string memory
3 _ha) public {
4     Student storage std = p[a];
5     std.name = sname;
6     std.course = scourse;
7     std.attendance = atte;
8     std.institutenam = inst;
9     std.c_id= _cid;
10    std.datetime=dt;
11    std.status = _Sta;
12    std.hash = _ha;
13}

```

(a)

```

1 function getDetails(address a) public view returns(address, string memory , string memory,
2 string memory,string memory,string memory,string memory,
3 string memory ,string memory){
4     Student storage std = p[a];
5     return(a,std.name , std.course,std.attendance , std.institutenam, std.c_id,
6         std.datetime, std.status,std.hash);
7}

```

(b)

```

1 pragma solidity ^0.5.2;
2 pragma experimental ABIEncoderV2;
3 contract Digial_Certificate{
4 struct Student{
5     string name;
6     string course;
7     string attendance;
8     string institutenam;
9     string c_id;
10    string datetime;
11    string status;
12    string hash;
13}
14 mapping(address => Student) public p;
15 function verify(address a, string memory _status,
16 string memory _hash ) public view returns (address, string
17 memory , string memory,
18 string memory,string memory,string memory,
19 string memory,string memory ,string memory)
20 { Student storage std = p[a];
21
22 if(keccak256(abi.encodePacked(std.status)) ==
23 keccak256(abi.encodePacked(_status)))
24 {
25     if(keccak256(abi.encodePacked(std.hash)) ==
26 {
27         return(a,std.name , std.course,std.attendance ,
28             std.institutenam,
29             std.c_id, std.datetime, std.status,std.hash);}
30 }
31 }
32}

```

(c)

Figure 9. The smart contract design and functionality for managing student information with (a) the solid visualization of a smart contract structure showing how student details get added, (b) users can view complete specifics that exist within the smart contract code base, and (c) hash verification of the smart contract code operates as a data integrity check to protect both transaction security and prevent unauthorized tampering



Student Address	Student Name	Course Name	Institute Name	Attendance	Date	Status
0x0A098Eda01Ce92f4A4CCb7A4fFb5A43EBC70DC	Osama Ahmed	Blockchain	Udemy	Present	2022-03-09	Pending

Figure 10. Depicting the process of locally adding a record to a MySQL database, demonstrating the insertion of data into the database table

Student Address	Student Name	Student Course	Student Institute	Student Attendance	Student Date	Student Status	Action
0x0A098Eda01Ce92f4A4CCb7A4fFb5A43EBC70DC	Osama Ahmed	Blockchain	Udemy	Present	2022-03-09	Pending	<button>Update</button>
0x03C9FcED478cBc0a4FAB34eF940767736D1Ff7	Omer Zafar	Html	Coursea	Present	2022-03-06	Pending	<button>Update</button>
0xAb8483F949C8d1EcF9b849Ae977dD3315835cb2	Ahmed Ali	Fython	Ned	Present	2022-03-09	Active	<button>Update</button>
0x1aE0EA3a72D944a8C7603FB3eC30a866E454C	Asad Saleh	Asp .Net	Udemy	Present	2/24/2021	Active	<button>Update</button>
0x14723A09ACf8D2A80DcdF7aA4AF308FDDC160C	Alisha	Blockchain	Coursea	Present	12/12/2021	Active	<button>Update</button>
0x583031D1113aD414F02576BD8afaBfb302140225	Afnan	SEO	Udemy	Present	12/12/2020	Active	<button>Update</button>
0xd870f0A1b7C4700F2BD7f44238821C2e7392148	Kareem	php	Ned	Present	12/1/2020	Active	<button>Update</button>
Student Address	Student Name	Student Course	Student Institute	Student Attendance	Student Date	Student Status	Action

Figure 11. Showcasing the user interface for updating or viewing records within a web application, enabling users to interact with and manage data seamlessly

**Certificate of Completion**

This is to certify that

Student Name **Alisha**

has completed the course **Blockchain**

from the Institute of **Coursea**

dated **12/12/2021**

Hash **0x4ab698cc264637c54885356f2e594e947d343cc96d66d9c0c303369e2dccc94888**

Download

Figure 12. Depicting the process of generating a certificate and providing its corresponding hash value, demonstrating the secure issuance and verification of certificates

### 5.5. Student or verifier

Students nowadays obtain a variety of educational certifications. These certificates are produced by students when they seek jobs in the public or private industry, where they must manually validate all of these credentials. Recruiting firms must ensure that the educational certificates of their candidates are genuine. As a result, this module was created to allow recruiters to validate any certificate by submitting the obtained certificate file using an application interface. The application will begin by contacting the cooperative contract to accept the contract address of the appropriate smart contract. Companies or organizations can thus query the system for details on any certificate. The suggested method reduces administrative costs, avoids document counterfeiting, and offers accurate and reliable digital certificate information. Following are the features of Student or Verifier from any company. The student or verifier has the right to view student details, generate a certificate, verification of account hash, verify the certificate and download the certificate.

- View Details: in Figure 13, Students can see their status or details; if the status is pending, then the web application will not allow them to view the certificate; otherwise, it can be available and seen.

In Figure 14, students or verifiers can see the certificate and verify the hash at any time. View certificates shows a list of all the available certifications in a single account. To obtain and display all certificates, it scans each generated certificate contract from the blockchain using the transaction. In Figure 15, entering the student's address and hash the result will return the complete details of the student including the hash.

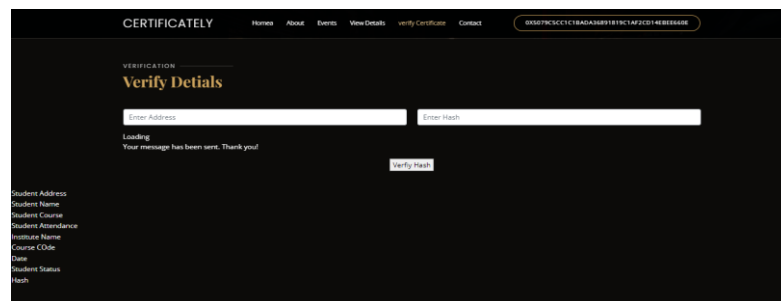


Figure 13. Illustrating the access of student status or details by verifiers through a web application, facilitating efficient verification processes

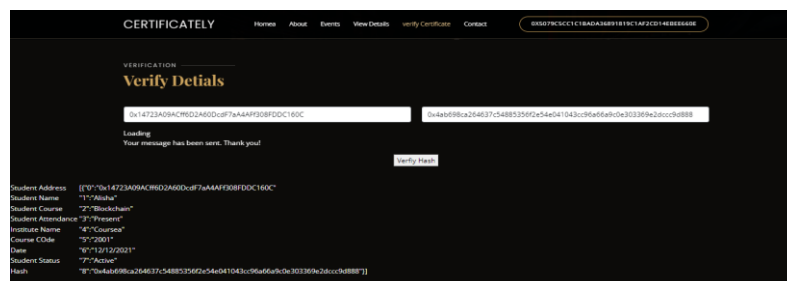


Figure 14. The hash verification process for student records, ensuring data integrity and authenticity within the educational system

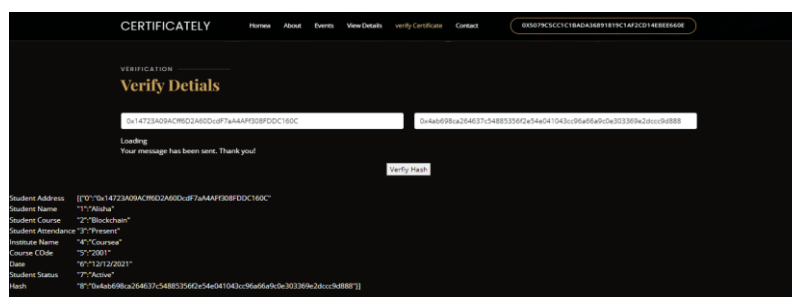


Figure 15. Confirming the successful hash verification of student records, ensuring the integrity and authenticity of the data within the educational system.

## 6. RESULTS AND DISCUSSION

The assessment features analysis of complete transaction duration alongside verification system efficiency which demonstrates system response speed and dependability performance. The evaluation presents findings about transaction time duration and verification accuracy which help determine both strong and weak points in the certificate handling system. The research seeks to create an accurate picture of how the system performs throughout different workloads and determine variables impacting digital certificate processing speed and accuracy.

### 6.1. Digital certificate transaction analysis

The university must first register to establish not modifiable credentials based on Blockchain. Who could send any transaction to the registered university's wallet address? Only the intelligent contract's owner has the right to make changes. The smart contract is deployed on the client side since Metamask authenticates the account. As a result, the contract must be published entirely the first time it is inserted; after that, contract methods can be used to get or update independent variables. Figure 16 depicts the process of confirming a transaction through MetaMask, a widely used Ethereum wallet browser extension, highlighting its role in facilitating secure and transparent blockchain interactions. The illustration showcases the user interface of MetaMask, where users are prompted to review transaction details before approval. Once the details are verified, the user approves the transaction by digitally signing it with their private key, which is securely stored within the MetaMask wallet. The transaction is then broadcast to the Ethereum blockchain for validation by the network's nodes. MetaMask enhances security by ensuring users have full control over their private keys and by providing a transparent overview of all transaction parameters, making it an essential tool for interacting with decentralized applications (dApps) and managing digital assets on the blockchain.

So, because smart contract coding has been released to the chain, such tasks require ether charge costs to complete, but they are typically much less expensive than the overall smart contract issuance. In Table 5 provides a detailed record of transactions, including timestamps, amounts, and participant identifiers, offering a clear and comprehensive transaction history. It ensures transparency by capturing key details such as transaction IDs, statuses, and the exact time of each interaction, supporting traceability and accountability in the system. Among the most crucial characteristics is that data immutability. It works as a large public ledger, with each intermediate node verifying and storing the same data.

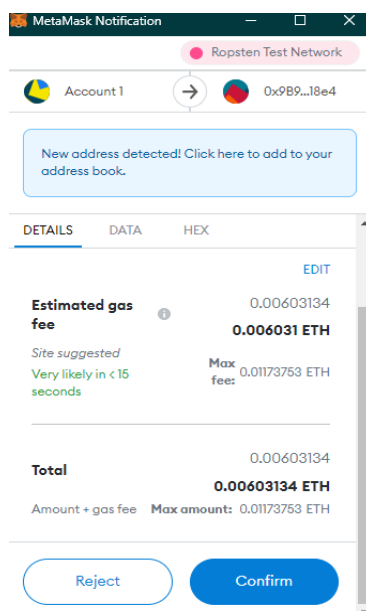


Figure 16. Illustration depicting the confirmation of a transaction through MetaMask, a popular Ethereum wallet browser extension, ensuring secure and transparent blockchain interactions

#### 6.1.1. Transaction time taken analysis

The duration required to produce a secure certificate through generate certificate method includes completing cryptographic operations and performing data integrity checks. Table 6 shows the breakdown between compilation time and actual execution duration for generate certificate and verification process

methods with additional assessment for certificate generation and validation improvements. The evaluation of method efficiency becomes possible through these results. We evaluate the duration needed for generate certificate functions as well as verification process operations. The time it takes to verify the generated certificate falls under the category of verification process time which ensures both authenticity and correct information. We achieve a better understanding of the proposed methods' computational performance and efficiency by comparing their processing times and thus we can identify areas that need optimization.

Table 5. Depicting the recording details of transactions, offering a comprehensive overview of transaction history, including timestamps, amounts, and participants

Blockchain technology	Fields	Description
Blockchain	ID	Blockchain Server identifier is represented public key
	Last Update	Most recent update time is shown by a timestamp.
	NetworkID	Network Address
	LastBlockNumber	The last block which the update procedure was run.
Transactions	Transactional Hash	Blockchain Server identifier is represented Hash.
	Institution Name	The Institution's account through transaction was sent.
	Gas Price	Transaction is going to the blockchain, the cost was charged.

Table 6. Detailed analysis and potential improvements for generating and verifying digital certificates

Method	Time taken	Suggested improvements
Compilation	<ul style="list-style-type: none"> <li>- To time: 180 seconds</li> <li>- Data Collection: 60 seconds</li> <li>- Encoding and Hashing: 70 seconds</li> <li>- Smart Contract Execution: 50 seconds</li> </ul>	<ul style="list-style-type: none"> <li>- The data encoding process should be optimized because it affects hashing duration.</li> <li>- Parallel processing for data collection.</li> <li>- The system should optimize smart contract execution to boost speed in processing.</li> </ul>
Generate Certificate	<ul style="list-style-type: none"> <li>Total time: 60 seconds</li> <li>- The execution of the smart contract inserts certificate data and hash into storage.</li> <li>- The system applies distinctive hash values to the digital certification.</li> </ul>	<ul style="list-style-type: none"> <li>- Improve smart contract efficiency.</li> <li>- Layer-2 solutions such as Polygon can minimize transaction speeds for the system.</li> <li>- Enhance blockchain fees together with processing speed.</li> </ul>
Verification	<ul style="list-style-type: none"> <li>Total time: 60 seconds</li> <li>- The system retrieves hash records from the blockchain storage system.</li> <li>- The verification system checks the submitted certificate hash against the stored hash on record.</li> <li>- Confirming authenticity.</li> </ul>	<ul style="list-style-type: none"> <li>- The storage system uses indexes to enable faster data retrieval operations.</li> <li>- Optimize hash comparison algorithm.</li> <li>- Store data in cache because it experiences frequent access.</li> </ul>
Performance Metrics	<ul style="list-style-type: none"> <li>- Throughput: The system generates certificates at a rate of per second.</li> <li>- Transaction Success Rate: Percentage of successful certificate generation attempts.</li> <li>- Network Latency: It defines the processing time for data both during transmission and computation phases</li> </ul>	<ul style="list-style-type: none"> <li>- The system needs processing enhancements to produce increased throughput.</li> <li>- The network infrastructure should receive optimization for latency reduction.</li> <li>- Failed transactions should be automatically retried during the process.</li> </ul>
Scalability	The system maintains peak performance levels while conducting large numbers of transactions.	<ul style="list-style-type: none"> <li>- The system requires testing under conditions of maximum load.</li> <li>- The system can scale capacity through horizontal scaling techniques.</li> <li>- Load balancing distribution methods should be implemented for processing task allocation.</li> </ul>
Comparison with Existing Systems	<ul style="list-style-type: none"> <li>Traditional systems provoke slower and less protected transactions because they need centralized servers.</li> <li>Blockchains improve both system transparency and security however they should expect longer processing durations.</li> </ul>	<ul style="list-style-type: none"> <li>- Examine transaction speeds together with costs in relation to current business systems.</li> <li>- The system needs an updated interface to attract more users.</li> <li>- Balance security and speed.</li> </ul>
Potential Optimization Areas	<ul style="list-style-type: none"> <li>- Reduce compilation and verification time.</li> <li>- Improve smart contract execution time.</li> <li>- Users will experience better interaction through shortened response delays.</li> </ul>	<ul style="list-style-type: none"> <li>- The system should maximize its capabilities for data handling as well as processing operations.</li> <li>- The application of machine learning models should both forecast and prepare incoming data.</li> <li>- Minimize transaction costs through batching.</li> </ul>
Security vs. Speed Trade-off	The security level rises as encryption strength increases together with complex zero-knowledge proof systems which results in processing time extensions.	<ul style="list-style-type: none"> <li>- The system should balance its encryption level against its processing speed parameters.</li> <li>- The research should investigate alternative cryptographic approaches to attain faster processing times.</li> </ul>
User Experience Impact	The duration of 5-minute processing time might impact how satisfied users feel when they submit numerous requests.	<ul style="list-style-type: none"> <li>- The system should accomplish processing under 3 minutes duration.</li> <li>- Users should get current processing updates in real time.</li> <li>- The system allows batch processing for big requests from multiple users.</li> </ul>

### 6.1.2. Verification process

The `verifyCertificate()` method of the contract function performs authentication validation for submitted certificates. A cryptographic hash computation of the certificate initiates before the method checks the stored hash values in the smart contract. Verification of the certificate depends on whether the computed hash matches any of the stored hashes in the system. Secure hashing algorithms employed during the verification process protect both stability and validity of the certificate by making it immune to unauthorized modifications. The verification system simultaneously handles several certificate submissions until completion but its processing duration depends on the current number of certificates submitted. The verification process takes longer when more certificates need to be verified since the increased computational workload involves executing smart contract functions and comparing several hashes. The methodology ensures that secure authorizations from legitimate sources are authorized for the system which boosts reliability and security.

## 7. PERFORMANCE ANALYSIS

Blockchain is gaining traction in academia and industry, as it is seen as a game changing technology that has the potential to help a wide range of industries. We used transaction scripts to inject transactions into the system after introducing modules inside the test setup. The gas consumption of these functions was profiled. However, despite the immense excitement surrounding blockchain, it's crucial to acknowledge that we are likely nearing the peak of inflated ex-pectations. While the technology holds immense potential, it's important to temper dis-cussions with a realistic understanding of its current limitations. In Figure 17 provides a comprehensive analysis of the performance metrics related to certificate issuance and verification rates per second within a blockchain framework. Figure 17(a) illustrates the fluctuations in these rates, highlighting variations influenced by system activity and load. Figure 17(b) showcases the dynamic nature of transaction validation, emphasizing how changes in network traffic impact processing efficiency. Figure 17(c) delves deeper into the subtle shifts in issuance and verification rates, exploring the complex relationship between verification mechanisms and associated gas fees. Finally, Figure 17(d) examines the combined effect of verification processes and gas fees on transaction throughput, offering valuable insights into the real-time behavior of the system under varying operational conditions. Together, these figures underscore the interplay between system performance, gas costs, and network dynamics, providing a detailed understanding of blockchain-based certificate management.

Through such endeavors, academia and industry can work together to en-sure blockchain fulfills its true potential to revolutionize various sectors. In Figure 18 provides a detailed analysis of the relationship between the number of certificates processed and the time required for different stages of the blockchain-based system. In Figure 18(a), illustrates how the estimation time varies with the number of certificates, reflecting the time required to predict and prepare the computational resources needed for certificate issuance and verification. Figure 18(b) focuses on the execution time, showcasing the actual time taken to complete the certificate issuance and verification processes. As the number of certificates increases, the estimation time typically grows, indicating the scalability challenges and resource allocation demands. This metric provides insight into the system's operational efficiency, revealing how performance scales with workload. Together, these figures highlight the system's capability to handle increasing workloads, while also identifying areas where optimization may be needed to enhance efficiency and reduce delays.

Blockchain is gaining traction in academia and industry, as it is seen as a game-changing technology that has the potential to help a wide range of sectors near the apex of unrealis-tic expectations, recognising the zeal with which this technology is currently widely dis-cussed in the media. After introducing modules into the test configuration, we deployed transaction scripts to insert transactions into the system.

In Table 7 provides a comprehensive overview of the latest gas fees on the Ethereum network, offering users real-time data to assist in transaction planning and cost management. The system analysis unfolds with enhanced performance evaluations which include measurement of success rates together with error rates and assessments of scalability alongside security factors. The table tracks fluctuations in gas prices, which can vary depending on network congestion and transaction demand. It includes key metrics such as the current average gas price (measured in gwei), historical trends, and peak fee periods, enabling users to identify the most cost-effective times to execute transactions. The results are provided in the next section, which profiles the gas consumption of these functions.

The relationship between the number of registrations and the number of certificates issued. In Figure 19 the bars represent the total number of registrations at each certificate level, demonstrating a clear positive correlation where higher certificate levels correspond to increased registrations. The black error bars indicate the variability or uncertainty in the data, reflecting the range of possible registration values. This trend suggests that as more certificates are introduced or made available, the number of user registrations tends to increase proportionally, highlighting the growing demand for academic credential verification.

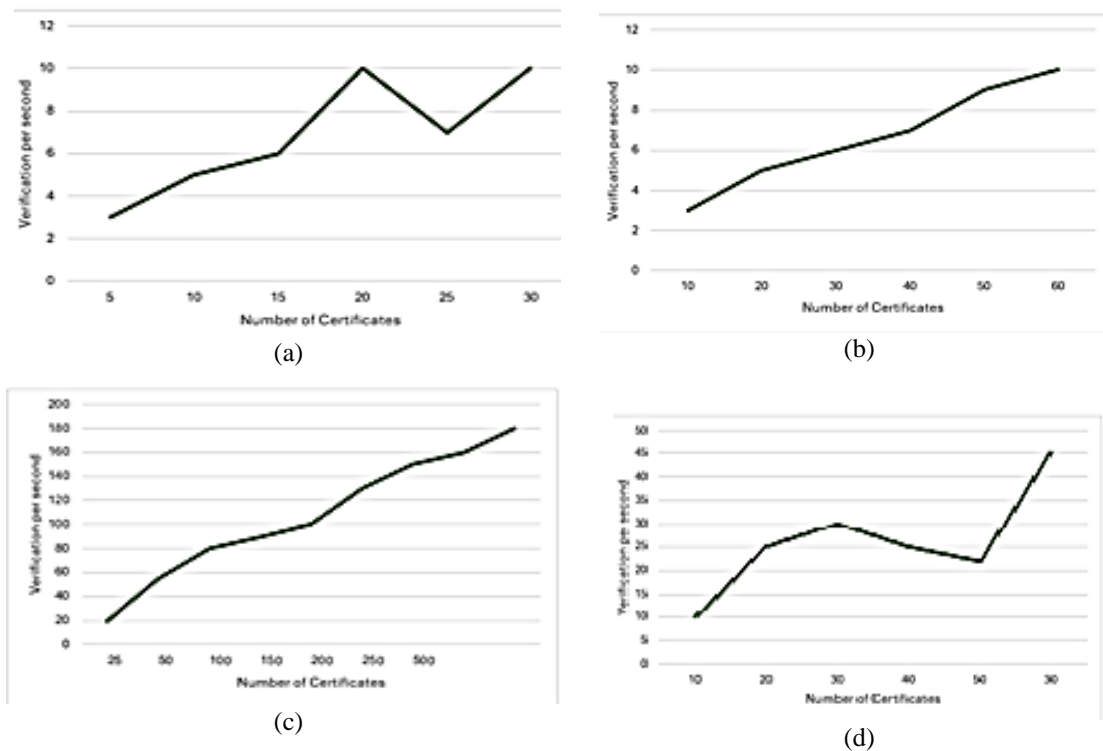


Figure 17. A comprehensive analysis of performance metrics related to certificate issuance and verification rates per second within a blockchain framework: (a) illustrates fluctuations in certificate issuance and verification rates per second, (b) reflecting the dynamic nature of transaction validation, (c) captures the nuanced changes in certificate issuance and verification rates per second, shedding light on the intricate interplay between verification processes and gas fees, and (d) reveals the influence of verification procedures and gas fees on certificate issuance and verification rates per second, offering insights into the real-time dynamics of transaction validation

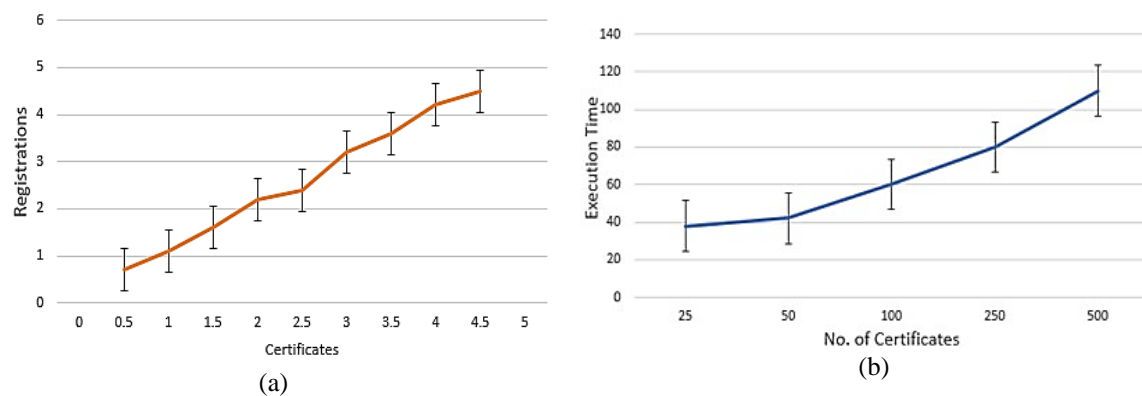


Figure 18. Comparson between no. of (a) certificate vs (b) execution time

Verification rate per number of certificates for three different verification methods (A, B, and C). In Figure 20 represents the number of verifications per second, while on the other side number of certificates being processed. Verification C consistently achieves the highest rate, followed by verification A and verification B, indicating that verification C is more efficient in handling higher volumes of certificates.

The relationship between gas fees and transaction volume, highlighting how the cost of processing transactions varies with the volume of transactions. The chart demonstrates that gas fees tend to increase progressively as transaction volume rises, reflecting the impact of higher network congestion and resource demand on transaction costs. The use of dark colors enhances the contrast, making it easier to distinguish

between different data points. The trend shown in the chart aligns with the hypothesis that higher transaction volumes can lead to increased gas fees due to greater competition for network resources. This insight underscores the importance of optimizing transaction processing through mechanisms such as layer-2 solutions, batching, and efficient encoding to minimize gas costs while maintaining performance. Understanding this relationship can help improve the system's scalability and reduce the financial burden on users, particularly during peak network activity.

A detailed comparison between the initial hypotheses and the actual results obtained from the academic credential verification system. The Table 8 outlines key performance metrics, including transaction time, efficiency, verification accuracy, security, gas fees, scalability, performance under load, user experience, and optimization. While the system met expectations in terms of security, verification accuracy, and overall stability, some areas showed room for improvement. For instance, transaction times were longer than anticipated due to the complexity of smart contract compilation, indicating the need for optimization through parallel processing and improved encoding. Similarly, scalability and efficiency were maintained under load, but minor bottlenecks emerged, suggesting that layer-2 solutions and better contract execution strategies could enhance performance. Verification accuracy was high, but processing speed declined under heavy load, highlighting the importance of indexed storage and caching. In Figure 21 Security measures ensured data integrity but caused processing slowdowns, indicating a need for more efficient cryptographic methods. User experience was positive, but the overall processing time of approximately five minutes could be shortened to improve customer satisfaction, potentially through batch processing and enhanced system responsiveness. These insights provide a clear roadmap for future improvements, ensuring a more efficient, secure, and user-friendly system.

Table 7. The analysis reveals performance metrics regarding digital certificate operations including execution time, operational success rates, system scalability and protection effects during registration, proofing and retrieval stages

Method	Time taken	Success rate (%)	Load handling	Scalability	Gas fee	Error rate (%)	Security impact
Register for a credential account.	0.006031	99.5%	High	Linear increase with load	Minimal	0.5%	The process of registration becomes secure because of encryption along with hashing techniques that maintain data integrity.
Proof of certificates	0.006045	99.2%	High	Linear increase with load	Minimal	0.8%	Using secure hash comparison helps prevent both forgery attempts and unauthorized tampering of data.
Retrieve certificates	No Gas Fee	99.8%	Very High	The system maintains minimal impact because it operates in read-only mode.	None	0.2%	The system implements encryption techniques for retrieval operations which deliver both confidentiality and integrity guarantee.

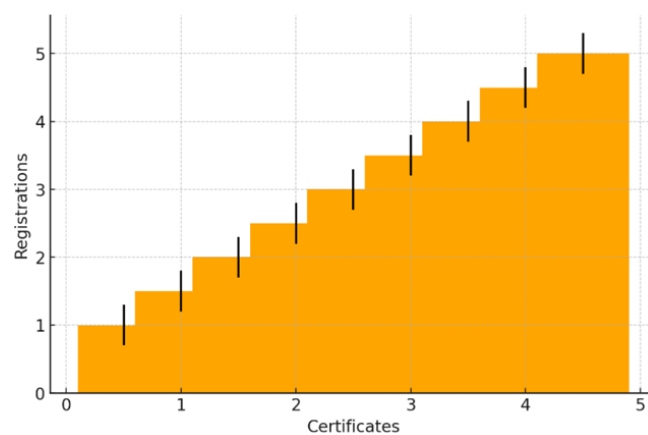


Figure 19. Registrations versus certificates, showing a positive correlation with error bars indicating variability



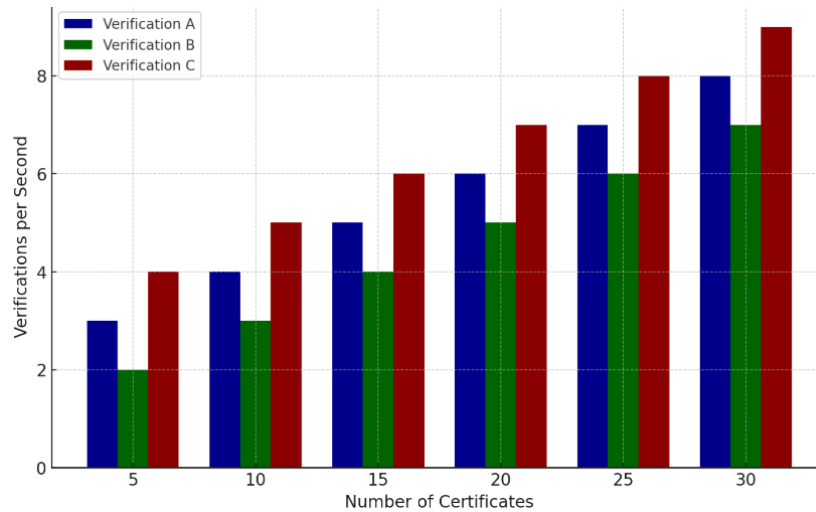


Figure 20. Verification rate per number of certificates for three methods, showing Verification C as the most efficient

Table 8. Comparison between initial hypotheses and actual results, highlighting insights and potential improvements in the academic credential verification system

Category	Initial Hypothesis	Results	Insights	Potential improvements
Transaction Time	The execution speed is accelerated because of automatic smart contract functionality.	Generate: 60s, Verification: 60s, Compilation: 180s	The system fulfills requirements although it takes a prolonged time to compile	Optimize encoding, use parallel processing
Efficiency	High efficiency under load	The system processed great numbers while experiencing minimal performance interruptions.	Efficient but bottlenecks under load	Use layer-2 solutions, improve contract execution
Verification	Fast and accurate	99.2% proofing, 99.8% retrieval	High accuracy, slower under heavy load	The system should implement indexed storage together with caching and optimization of comparison results.
Security	High integrity and protection	Secure and resistant to tampering	Periods of increased processing times occur because of encryption measures during the operation.	Explore faster cryptographic methods
Gas Fees	Moderate, influenced by network congestion	Registration: 0.006031 ETH, Proofing: 0.006045 ETH	Payment expenses stay affordable but experience changes according to network utilization levels.	Use layer-2, implement batching
Scalability	Consistent under high volume	Linear increase in processing time	Stable but slower under peak load	Horizontal scaling, load balancing
Performance Under Load	Stable throughput and response time	High success rate, minor fluctuations	Stable but slower with high traffic	Increase processing power, optimize network
User Experience	Smooth with fast response	The workflow requires approximately 5 minutes for completion while status notifications are delivered during the process.	Longer time may affect satisfaction	Customers need their documents processed within 3 minutes while batch processing should be enabled.
Traditional Systems	Faster and more secure	Better security, slightly slower speed	Improved security, but slower processing	Improve speed without reducing security
Optimization	Identify improvement areas	Bottlenecks in encoding and processing	Clear areas for enhancement	Optimize data handling, reduce costs

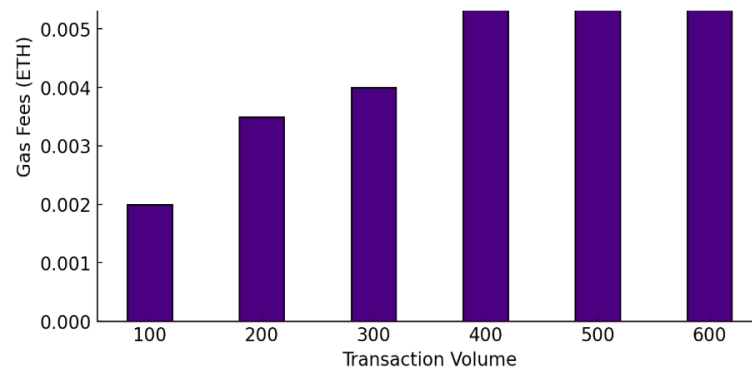


Figure 21. The relationship between gas fees and transaction volume, highlighting the trend of increasing costs with higher transaction volumes

## 8. CONCLUSION AND FUTURE WORK

Developing an academic credentials verification system is still in its early stages. Many ways in which we can further develop this project. Developing an academic credentials verification system is still in its early stages. Many ways in which we can further develop this project. Here are some possible areas of future work: Another potential area for development is creating a more user-friendly interface. A modern academic credentials verification system needs development for present-day educational and employment requirements because fraudulent academic certificates have become a major obstacle. Academic credential authentication demands blockchain technology as a solution to establish unalterable transparent credentials verification procedures. This paper develops CERTIFICATELY as a blockchain system that enables smart contracts to streamline certificate issuance while showcasing how blockchain can protect security and stop tampering and strengthen verification speed. The study demonstrates that blockchain technology lowers administrative expenses effectively and enhances academic qualification trustworthiness alongside its ability to handle large volumes of transactions. Although users expressed minor time-related processing issues and fee concerns regarding the solution the high success rate combined with scalability proves the effectiveness of this approach. The user-friendly interface of CERTIFICATELY coupled with MetaMask integration eliminates the concerns related to system complexity and technical requirements among critics. Building on existing developments should focus on fastening smart contract performance and adopting layer-2 solutions like Polygon to cut down gas fees. System adoption alongside user satisfaction will grow as the interface becomes more accessible to multiple users. It uses for educational systems can be grouped into numerous categories due to this assessment process in various articles and papers, such as a decentralised publicly dispersed educational system.

This research focuses on apps that have been created for educational objectives, which are assessed for their purpose and implementation technique, as well as issues that must be resolved in future functionality. The uses for educational systems can be grouped into numerous categories due to this assessment process in various articles and papers, such as a decentralised publically dispersed educational system. A world-wide database of approved institutions should be established to simplify the verification process and decrease fraud vulnerability. The system functionality plus practical industry value will grow by including third-party verification features and extending the platform to verify both professional and vocational credentials. The investigation creates basic principles for blockchain academic verification system development which enables establishment of a trustworthy credentialing structure for the future.

## ACKNOWLEDGMENTS

The authors show their deep appreciation toward the Department of Computer Science and IT at NED University of Engineering and Technology in Pakistan for their valuable assistance.

## FUNDING INFORMATION

The authors did not receive any financial support from external entities for this project.

### AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Umna Iftikhar	✓	✓	✓	✓	✓				✓	✓			✓	
Hafiz Muhammad Attallah		✓							✓	✓	✓	✓		
Inam Ullah Khan	✓		✓	✓					✓		✓		✓	
Muhammad Mansoor Alam	✓	✓					✓		✓			✓	✓	
Mazliham Mohd Su'ud					✓		✓			✓		✓		
Ahthasham Sajid					✓		✓			✓	✓	✓	✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

### CONFLICT OF INTEREST STATEMENT

The authors report having no potential financial or non-financial biases.




### REFERENCES

- [1] G. Maulani, G. Gunawan, L. Leli, E. Ayu Nabila, and W. Yestina Sari, "Digital certificate authority with blockchain cybersecurity in education," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 136–150, May 2021, doi: 10.34306/ijcitsm.v1i1.40.
- [2] K. Kumutha and S. Jayalakshmi, "Blockchain technology and academic certificate authenticity—a review," in *Lecture Notes in Networks and Systems*, vol. 209, Springer Singapore, 2022, pp. 321–334.
- [3] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: Research and Applications*, vol. 3, no. 2, p. 100067, Jun. 2022, doi: 10.1016/j.bcr.2022.100067.
- [4] R. Q. Castro and M. Au-Yong-oliveira, "Blockchain and higher education diplomas," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, no. 1, pp. 154–167, Feb. 2021, doi: 10.3390/ejihpe11010013.
- [5] A. R. Sathya, S. K. Panda, and S. Hanumanthakari, "Enabling smart education system using blockchain technology," in *Intelligent Systems Reference Library*, vol. 203, Springer International Publishing, 2021, pp. 169–177.
- [6] L. Asiri, "Blockchain for educational certificate distribution," *PhD thesis*, 2020.
- [7] J. Xu, C. Wang, and X. Jia, "A survey of blockchain consensus protocols," *ACM Computing Surveys*, vol. 55, no. 13s, pp. 1–35, Jul. 2023, doi: 10.1145/3579845.
- [8] F. Saleh, "Blockchain without waste: proof-of-stake," *SSRN Electronic Journal*, 2018, doi: 10.2139/ssrn.3183935.
- [9] A. Altarawneh, F. Sun, R. R. Brooks, O. Hambolu, L. Yu, and A. Skjellum, "Availability analysis of a permissioned blockchain with a lightweight consensus protocol," *Computers and Security*, vol. 102, p. 102098, Mar. 2021, doi: 10.1016/j.cose.2020.102098.
- [10] S. Bano *et al.*, "Sok: Consensus in the age of blockchains," in *AFT 2019 - Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, Oct. 2019, pp. 183–198, doi: 10.1145/3318041.3355458.
- [11] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020, doi: 10.1109/COMST.2020.2969706.
- [12] S. Aggarwal and N. Kumar, "Hyperledger," in *Advances in Computers*, vol. 121, Elsevier, 2021, pp. 323–343.
- [13] A. A. Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission," *Applied Sciences (Switzerland)*, vol. 11, no. 22, p. 10917, Nov. 2021, doi: 10.3390/app112210917.
- [14] M. Almakhour, L. Sliman, A. E. Samhat, and A. Mellouk, "Verification of smart contracts: A survey," *Pervasive and Mobile Computing*, vol. 67, p. 101227, Sep. 2020, doi: 10.1016/j.pmcj.2020.101227.
- [15] Z. Zheng *et al.*, "An overview on smart contracts: Challenges, advances and platforms," *Future Generation Computer Systems*, vol. 105, pp. 475–491, Apr. 2020, doi: 10.1016/j.future.2019.12.019.
- [16] S. Sunitha kumari and D. Saveetha, "Blockchain and smart contract for digital document verification," *International Journal of Engineering & Technology*, vol. 7, no. 4.6, p. 394, Sep. 2018, doi: 10.14419/ijet.v7i4.6.28449.
- [17] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba, and O. Said, "Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 10, pp. 4639–4649, Sep. 2022, doi: 10.1007/s12652-021-03459-4.
- [18] G. Srivastava, S. Dhar, A. D. Dwivedi, and J. Crichigno, "Blockchain education," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019*, May 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861828.
- [19] P. P. Pittalia, "A comparative study of hash algorithms in cryptography," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 6, pp. 147–152, 2019.
- [20] T. Phillips, R. K. Saunders, J. Cossman, and E. Heitman, "Assessing trustworthiness in research: A pilot study on CV verification," *Journal of Empirical Research on Human Research Ethics*, vol. 14, no. 4, pp. 353–364, Jul. 2019, doi: 10.1177/1556264619857843.
- [21] K. Clements, R. E. West, and E. Hunsaker, "Getting started with open badges and open microcredentials," *The International Review of Research in Open and Distributed Learning*, vol. 21, no. 1, pp. 154–172, 2020.





- [22] S. Brauer, A. M. Korhonen, and P. Siklander, "Online scaffolding in digital open badge-driven learning," *Educational Research*, vol. 61, no. 1, pp. 53–69, Jan. 2019, doi: 10.1080/00131881.2018.1562953.
- [23] J. C. Cheng, N. Y. Lee, C. Chi, and Y. H. Chen, "Blockchain and smart contract for digital certificate," in *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, Apr. 2018, pp. 1046–1051, doi: 10.1109/ICASI.2018.8394455.
- [24] P. Panagiotidis, "Blockchain in education - the case of language learning," *European Journal of Education*, vol. 5, no. 1, pp. 66–82, Apr. 2022, doi: 10.26417/443gjm83.
- [25] J. A. Noyes, P. M. Welch, J. W. Johnson, and K. J. Carbonneau, "A systematic review of digital badges in health care education," *Medical Education*, vol. 54, no. 7, pp. 600–615, Mar. 2020, doi: 10.1111/medu.14060.
- [26] V. Chukowry, G. Nanuck, and R. K. Sungkur, "The future of continuous learning—Digital badge and microcredential system using blockchain," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 355–361, Nov. 2021, doi: 10.1016/j.gltp.2021.08.026.
- [27] A. Kamišalić, M. Turkanović, S. Mrdović, and M. Heričko, "A preliminary review of blockchain-based solutions in higher education," in *Communications in Computer and Information Science*, Springer International Publishing, 2019, pp. 114–124.
- [28] L. M. Palma, M. A. G. Vigil, F. L. Pereira, and J. E. Martina, "Blockchain and smart contracts for higher education registry in Brazil," *International Journal of Network Management*, vol. 29, no. 3, Jan. 2019, doi: 10.1002/nem.2061.
- [29] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3, pp. 79–84, Jan. 2020, doi: 10.31838/jcr.07.03.13.
- [30] R. Raimundo and A. Rosário, "Blockchain system in the higher education," *European Journal of Investigation in Health, Psychology and Education*, vol. 11, no. 1, pp. 276–293, Mar. 2021, doi: 10.3390/ejihpe11010021.
- [31] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, "Design framework on tertiary education system in indonesia using blockchain technology," in *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*, Nov. 2019, pp. 1–4, doi: 10.1109/CITSM47753.2019.8965380.
- [32] U. Iftikhar, M. Anwer, R. Butt, and G. Ahmed, "Towards 5G, 6G and 7G sustainable and potential applications using blockchain: comparative analysis and prospective challenges," in *2023 4th International Conference on Computing, Mathematics and Engineering Technologies: Sustainable Technologies for Socio-Economic Development, iCoMET 2023*, Mar. 2023, pp. 1–7, doi: 10.1109/iCoMET57998.2023.10099241.
- [33] A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *Journal of Information Security and Applications*, vol. 80, p. 103678, Feb. 2024, doi: 10.1016/j.jisa.2023.103678.
- [34] J. Ahn, E. Yi, and M. Kim, "Blockchain consensus mechanisms: a bibliometric analysis (2014–2024) using VOSviewer and R Bibliometrix," *Information (Switzerland)*, vol. 15, no. 10, p. 644, Oct. 2024, doi: 10.3390/info15100644.
- [35] Y. Chen, L. Yang, Y. Fan, L. Zhang, and L. Tian, "Study on energy efficiency and carbon neutral path of Ethereum blockchain: from PoW to PoS," in *Ninth International Conference on Energy Materials and Electrical Engineering (ICEMEE 2023)*, Feb. 2024, p. 28, doi: 10.1117/12.3015149.
- [36] V. B. Mišić, S. Naderi Mighan, J. Mišić, and X. Chang, "Decentralization is good or not? defending consensus in ethereum 2.0," *Blockchains*, vol. 2, no. 1, pp. 1–19, Jan. 2024, doi: 10.3390/blockchains2010001.
- [37] A. Petcu, B. Pahontu, M. Frunzete, and D. A. Stoichescu, "A secure and decentralized authentication mechanism based on web 3.0 and ethereum blockchain technology," *Applied Sciences (Switzerland)*, vol. 13, no. 4, p. 2231, Feb. 2023, doi: 10.3390/app13042231.
- [38] Z. Wang et al., "Robust permissioned blockchain consensus for unstable communication in FANET," *IEEE/ACM Transactions on Networking*, vol. 32, no. 1, pp. 699–712, Feb. 2024, doi: 10.1109/TNET.2023.3295378.
- [39] W. Liang, Y. Liu, C. Yang, S. Xie, K. Li, and W. Susilo, "On identity, transaction, and smart contract privacy on permissioned and permissionless blockchain: a comprehensive survey," *ACM Computing Surveys*, vol. 56, no. 12, pp. 1–35, Jul. 2024, doi: 10.1145/3676164.
- [40] R. Bezuidenhout, W. Nel, and J. M. Maritz, "Permissionless blockchain systems as pseudo-random number generators for decentralized consensus," *IEEE Access*, vol. 11, pp. 14587–14611, 2023, doi: 10.1109/ACCESS.2023.3244403.
- [41] S. Atanov, Y. Seitkulov, K. Moldamurat, B. Yergaliyeva, A. Kyzrkanov, and Z. Seitbatalov, "About one lightweight encryption algorithm ensuring the security of data transmission and communication between internet of things devices," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 6, pp. 6861–6873, Dec. 2024, doi: 10.11591/ijece.v14i6.pp6846-6860.
- [42] F. Nabi, X. Zhou, U. Iftikhar, and H. M. Attaullah, "A case study of cyber subversion attack based design flaw in service oriented component application logic," *Journal of Cyber Security Technology*, vol. 8, no. 3, pp. 204–228, Oct. 2024, doi: 10.1080/23742917.2023.2261169.
- [43] A. Jumagaliyeva et al., "The impact of blockchain and artificial intelligence technologies in network security for e-voting," *International Journal of Electrical and Computer Engineering*, vol. 14, no. 6, pp. 6723–6733, Dec. 2024, doi: 10.11591/ijece.v14i6.pp6723-6733.

## BIOGRAPHIES OF AUTHORS







**Umna Iftikhar**    received her Master's degree in Information Security from NED University of Engineering and Technology (NEDUET), Pakistan. She is currently serving as a Senior Lecturer at Iqra University, Pakistan. With extensive experience in both academic and industrial domains, she has authored several publications in high-quality international scientific journals and conference proceedings. Her research interests include cybersecurity, data privacy, artificial intelligence, and she remains actively engaged in contributing to advancements in her field. She can be contacted at email: yamnaiftikhar@gmail.com.







**Hafiz Muhammad Attaullah**     is a seasoned Cybersecurity Advocate/Red Team researcher. He has done his Bachelors (Hons) degree in Telecommunication Engineering, and MS (specialization in Cybersecurity) from NED University of Engineering and Technology, Pakistan. Currently doing PhD in Computing from Multimedia University Malaysia. He is the founder of four infosec products and patents, funded by Ignite and HEC. Currently he is working as Lecturer of Cyber Security at Department of Computer Science, Mohammad Ali University (MAJU), Karachi Pakistan. Also, he had the experience and the winner of many international Competitions. He is also serving as section secretary of IEEE Computer Society Karachi. His area of research includes SecOps, UAVs and ML for Security. He can be contacted at email: attaulahshafiq10@gmail.com.







**Dr. Inam Ullah Khan**     is a distinguished academic and industry leader, celebrated for his extensive contributions to Artificial Intelligence, Artificial General Intelligence, Unmanned Aerial Vehicles, Routing Protocols, Intrusion Detection Systems, Machine Learning, Deep Learning, and Evolutionary Computing. These include memberships in the International Association of Engineers (IAENG). He is currently working as Postdoctoral Research Fellow at Multimedia University, Malaysia. Also, Dr. Khan is Adjunct Faculty at PSGR Krishnammal College for Women, College in Coimbatore, India. In recognition of his expertise, Dr. Khan has frequently appeared on Pakistan National Television as a technology expert, further cementing his reputation as a thought leader. He can be contacted at email: inamullahkhan05@gmail.com.







**Prof. Dr. Muhammad Mansoor Alam**     received the M.S. degree in system engineering, the M.Sc. degree in computer science, the Ph.D. degree in computer engineering, and the Ph.D. degree in electrical and electronics engineering in France, U.K., and Malaysia, respectively, and the Très Honorable degree (Hons.) from Universite de LaRochelle. He was the Associate Dean of CCSIS and the Head of the Department of Mathematics, the Department of Statistics, and the Computer Science Department, IoBM, Pakistan. He is recently associated with Riphah International University, Islamabad. He is currently a professor in computer science. He can be contacted at email: m.mansoor@riphah.edu.pk.



**Prof. Dato' Dr. Mazliham Mohd Su'ud**     received the master's degree in electrical and electronics engineering from the University of Montpellier, in 1993, and the Ph.D. degree in computer engineering from Université de La Rochelle, in 2007. From 2013 to 2020, he was the President/CEO of Universiti Kuala Lumpur, Malaysia. Since 2020, he has been the President/CEO and professor of Multimedia University, Malaysia. He has vast experience in publishing articles in high-quality international scientific journals and conference proceedings. He has numerous years of experience in the industrial and academic fields. He can be contacted at email: mazliham@mmu.edu.my.



**Dr. Ahthasham Sajid**     is an HEC Approved Supervisor and currently working as "Assistant Professor" in Department of Cyber Security in Riphah Institute of System Engineering, Islamabad Pakistan, previously served as Assistant Professor under department of Computer Science in BUITEMS Quetta from 2010 to 2023. He has also served as HOD for 5 years; I have done PhD in Computer Science in year 2020 from SZABIST, Islamabad Pakistan. Their areas of interest are Wireless & Sensor Networks (VANET, MANETS, and UAVs), and Cyber Security. He has been serving as reviewer for IEEE Access, Wiley Software and Practice, MDPI, Springer and other well-renowned journals. He can be contacted at email: ahthasham.sajid@riphah.edu.pk.