Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

Veri-Scan: A Decentralized Approach to Academic Verification via RSA Cryptography and Dynamic Kill-Switches

Rohith PN
Dept. of Computer Science and Engineering
Christ (Deemed to be University)
Bangalore, India

Dr. Jyothi Mandala
Dept. of Computer Science and Engineering
Christ (Deemed to be University)
Bangalore, India

***Abstract*—The fake degree market has evolved from simple photoshopped edits to sophisticated forgeries that are increasingly difficult to spot. For educational institutions and recruiters, the verification process remains a significant bottleneck, often relying on slow, manual email exchanges that leave room for human error. While blockchain technology is frequently touted as the ultimate solution for document integrity, it brings its own set of problems: high transaction costs (gas fees) and slower confirmation times. In this paper, we introduce "Veri-Scan," a hybrid verification system that secures documents without the overhead of a full blockchain network. By combining Asymmetric Cryptography (RSA-2048) with SHA-256 hashing, we ensure data integrity and non-repudiation. Crucially, we introduce a novel "Kill Switch" mechanism—a database-level override that allows universities to revoke a certificate instantly, even after it has been downloaded or printed. Our full-stack implementation, built on Next.js, demonstrates that we can achieve verification speeds of under 0.8 seconds while maintaining 100% detection accuracy for tampered documents.**

***Index Terms*—Digital Signatures, RSA Cryptography, SHA-256, Document Verification, PKI, Kill Switch, EdTech.**

I. Introduction

Academic credentials are more than just paper; they represent the trust capital between a university, its students, and the job market. However, that trust is eroding. With the accessibility of advanced design software and AI tools, creating a convincing fake degree has never been easier. This places a heavy burden on recruiters, who must verify thousands of documents annually.

Currently, the National Academic Depository (NAD) in India is working to digitize these records, but private entities often face hurdles regarding API access and legacy data integration. Consequently, most recruiters fall back on the traditional method: emailing the university and waiting. This manual loop can take anywhere from a few days to a couple of weeks—a delay that often leads employers to skip the check entirely, creating a vulnerability that fraudsters exploit.

A. The Problem with Current Solutions

When we look at existing digital solutions, they tend to fall into two extremes:

1) **Centralized Databases:** These are fast but vulnerable. An internal bad actor with database access could potentially alter records without leaving a public trace.
2) **Blockchain Ledgers:** These are secure but expensive. Public chains like Ethereum require gas fees for every transaction. For a university issuing thousands of degrees, these costs add up quickly. Private blockchains, on the other hand, require complex infrastructure that many institutions are not equipped to maintain.

B. Our Contribution

We argue that you don't need a blockchain to get blockchain-like security. Veri-Scan is designed as a middle ground. We utilize the mathematical certainty of Public Key Infrastructure (PKI) to lock the data, while using a standard SQL database for speed and status management. Our key contributions include:

- A tamper-evident hashing mechanism using **SHA-256** that detects bit-level changes.
- A digital signing protocol using **RSA-2048** that proves the document's origin.
- A **Dynamic Kill-Switch**, which addresses a major flaw in static crypto-signatures: the inability to revoke a document once the private key has signed it.
- A frictionless mobile interface that allows verification without requiring the recruiter to log in or install an app.

II. Literature Review

The fight against document forgery isn't new, and several technological approaches have been tested.

Patil et al. [1] developed a QR-based system linked to Firebase. It was efficient for retrieving data, but it lacked a robust cryptographic layer. Essentially, the QR code was just a link. If a bad actor guessed the URL pattern, they could spoof the verification page entirely. Veri-Scan improves on this by embedding a cryptographic signature directly into the verification payload—without the key, you can't fake the QR code.

On the blockchain front, studies [2] have shown the immense value of decentralization. Ethereum smart contracts effectively make records immutable. However, the practical constraints—specifically fluctuating gas costs and network latency—make them hard to scale for day-to-day university operations. Additionally, strict data privacy laws (like the "Right to be Forgotten") can conflict with the permanent nature of blockchain. Our centralized database approach allows for regulatory compliance regarding data deletion while still securing the document content via cryptography.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

III. Methodology

We designed Veri-Scan around a three-phase lifecycle: Issuance, Access, and Verification.

A. System Architecture

We opted for a Monolithic Architecture using **Next.js 14**. This allows us to handle both the React frontend and the API routes in a single deployment, simplifying maintenance. For persistence, we use **MySQL** managed via **Prisma ORM**, which gives us type safety and fast query performance.

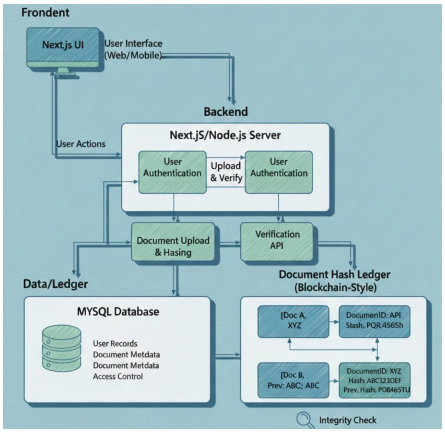

Fig. 1. System Architecture showing the data flow between Admin, Student, and Verifier.

The workflow involves three distinct actors:

1) **The Issuer (Admin):** Uses secure credentials to mint certificates.
2) **The Holder (Student):** Accesses their signed PDF via a portal using their Register Number and Date of Birth.
3) **The Verifier (Recruiter):** Scans the document to check its validity. Crucially, this step is permission-less—anyone with the QR code can verify it.

B. The Cryptographic Model

We chose the RSA-2048 standard because it offers a strong balance between security and processing speed on standard web servers.

Let M represent the student's data object:

$$M = \{\text{Name, RegNo, Course, GPA}\}$$

1) Hashing for Integrity: First, we run M through the SHA-256 algorithm.

$$h = H(M)$$

This creates a unique 256-bit digest. The "Avalanche Effect" here is critical: changing a GPA from 3.0 to 3.1 creates a completely unrecognizable new hash, instantly flagging any edits.

2) Signing for Authenticity: The university holds a private key (K_{priv}) that never leaves the secure server environment. We encrypt the hash h using this key:

$$S = E(h, K_{priv})$$

This signature S is the proof of origin. It can only be created by the university, but it can be read by anyone with the public key.

3) The Verification Logic: When a recruiter scans the QR code, the app receives the data (M') and the signature (S). 1. We decrypt S using the public key to see what the original hash was (h_{orig}). 2. We calculate the hash of the data currently on the paper (h_{curr}). 3. We compare them:

$$\text{Status} = \begin{cases} \text{Valid} & \text{if } h_{orig} == h_{curr} \\ \text{Tampered} & \text{if } h_{orig} \neq h_{curr} \end{cases}$$

C. The Kill Switch (Revocation)

Standard crypto-verification has a weakness: it works offline. If a university revokes a degree (perhaps due to malpractice found later), an offline verification of the old PDF would still pass because the math is still valid.

To close this loophole, we added a "Kill Switch." We maintain an `isRevoked` flag in our SQL database. Before returning a "Valid" status, the API performs a quick lookup. If the flag is raised, the system overrides the cryptographic check and forces a "Revoked" warning, regardless of the PDF's content.

Algorithm 1 Hybrid Verification Logic

Input: Data D, Signature S, Key K_{pub}
$h_{calc} \leftarrow \text{SHA256}(D)$
$h_{dec} \leftarrow \text{RSA\_Decrypt}(S, K_{pub})$
if $h_{calc} \neq h_{dec}$ **then**
  return RED (Tampered)
else
  $status \leftarrow$ DB.query(SELECT isRevoked FROM Certs WHERE regNo= $D.regNo$)
  if $status ==$ TRUE **then**
    return YELLOW (Revoked)
  else
    return GREEN (Valid)
  end if
end if

IV. Implementation & Results

The system was built on a standard MacBook Air M1 environment to test feasibility on consumer hardware.

A. Technology Stack

We utilized **Node.js** native libraries for the cryptography to avoid heavy external dependencies. For the frontend, **Tailwind CSS** allowed us to build a mobile-responsive scanner interface that works on any smartphone browser without installation.

B. Admin Workflow

The dashboard provides a simple interface for the Controller of Examinations. Upon clicking "Mint," the key generation and signing happen in milliseconds.

C. Security Testing

We ran specific attack vectors to ensure robustness:

1) **The Photoshop Attack:** We manually edited the PDF to change the name. The hash verification failed immediately, triggering the Red screen.
2) **The Replay Attack:** We tried copying a valid signature from one student to another. Since the signature is

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

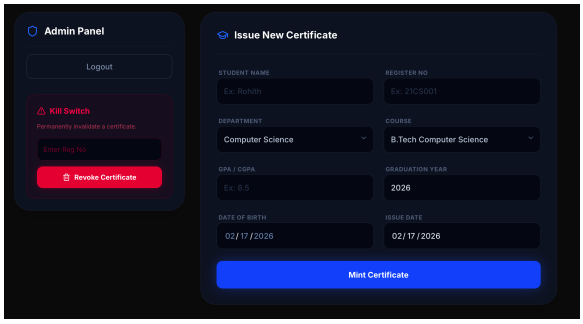

Fig. 2. The Admin Interface for issuing new credentials.

mathematically bound to the specific data of the first student, the decryption process produced a mismatch.

3) **The Revocation Test:** We marked a valid certificate as revoked. Even though the PDF was untouched, the scanner correctly identified the status change from the database.

D. Performance Benchmarks

Speed was a priority. We averaged the time taken over 50 trials.

TABLE I
SYSTEM LATENCY

Operation	Time (Avg)
Key Generation	210 ms
Signing Process	15 ms
PDF Generation	120 ms
Verify (Crypto Only)	5 ms
Total Verification Time	**0.8 sec**

A sub-second verification time is a massive improvement over blockchain solutions, which often require waiting for block confirmations.

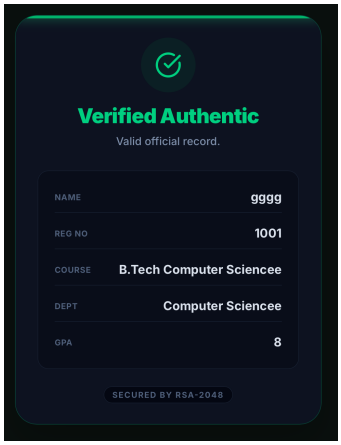

Fig. 3. Mobile Verification Screen showing a Valid Certificate.

E. Comparison

Table II breaks down how Veri-Scan stacks up against the alternatives.

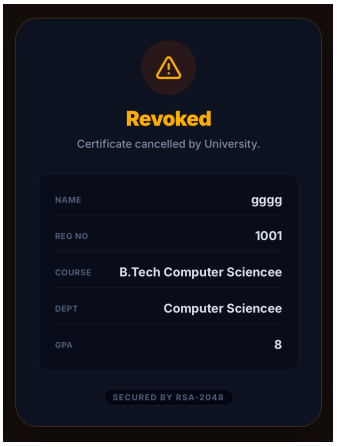

Fig. 4. Revocation Screen showing the Kill Switch in action.

TABLE II
COMPARISON OF VERIFICATION METHODS

Feature	Manual	Blockchain	Veri-Scan
Setup Cost	Low	High	Low
Transaction Cost	Low	High (Gas)	Zero
Verification Time	Days	Minutes	$<$ 1 Sec
Integrity	Low	High	High
Revocability	Difficult	Impossible	Instant

V. CONCLUSION

Veri-Scan proves that high-security document verification doesn't always require a blockchain. By intelligently combining RSA digital signatures for integrity and a centralized database for lifecycle management, we can offer universities a tool that is secure, fast, and remarkably cheap to run.

We addressed the "Trilemma" of cost, speed, and security. We achieved cryptographic assurance without the environmental or financial costs of a distributed ledger.

VI. FUTURE SCOPE

Moving forward, we aim to integrate this system with the **DigiLocker API** to ensure government compliance. We are also exploring **Batch Processing** features to allow universities to upload CSV files and mint thousands of degrees in a single click.

REFERENCES

[1] V. Patil, S. Sharma, and R. Gupta, "Digital Document Verification with QR Code using Firebase," *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, vol. 6, no. 4, pp. 120-125, 2024.
[2] A. Nasir, J. Khan, and M. Ali, "Development of QR Code-Based Authentication System for Examinations," *European Journal of Computer Science and Information Technology*, vol. 10, no. 3, 2025.
[3] S. Kumar, A. Singh, and P. Verma, "An Analytical Study on QR Code-Based E-Authentication," *NeuroQuantology*, vol. 19, no. 8, 2021.
[4] "Blockchain Based Certificate Authentication System," *IEEE Xplore Digital Library*, 2024.
[5] "Cloud-Based QR Code Authentication System for Real-Time Vehicle Verification," *International Journal for Modern Trends in Science and Technology (IJMTST)*, 2025.
[6] "Innovative QR Code System for Tamper-Proof Generation," *PMC Research*, 2025.
[7] "Authentication system for e-certificate by using RSA's digital signature," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 18, no. 2, 2020.