Grenze International Journal of Engineering and Technology, June Issue

Certificate Verification System Powered by De-Duplication and Supabase

Jane Rubel Angelina Jeyaraj[1], K. Sashank Reddy[2], K. Nanda Kesava[3], J. Jaswanth[4] and M. Abhilash[5]
[1-5]Kalasalingam Academy of Research and Education, Computer Science and Engineering, Krishnankoil, Tamilnadu, India
Email: j.janerubelangelina@klu.ac.in, j.janerubelangelina@klu.ac.in, kathisashank@gmail.com, Nandakesava1311@gmail.com, jasthijaswanth87@gmail.com, manuboluabhilash@gmail.com

***Abstract*— The increasing number of falsified and duplicated digital certificates is a colossal issue to institutions and organizations that attempt to determine the accuracy of academic and professional qualification. The traditional ways of validation are manual validation through issuance of authorities, which is not efficient in terms of time. As a solution to this issue, the provided paper proposes a safe protocol of digital certificates verification which will rely on the cryptography hash and data management using cloud-based data storage technologies to ensure certificate integrity and authenticity.**

The advanced framework will be to enable institutions to register and upload digital certificates through a safe interface. Each of the certificates is hashed using the hash-256 hash algorithm to get a unique digital representation of the certificate and this is in turn deduplicated by a deduplication mechanism to make known that the certificate is duplicated. When the certificate is unique, a verification ID is generated and the record of certificate is securely stored in the database. The Supabase PostgreSQL acts as a metadata storage and Supabase storage as a certificate file storage system that enables the placement of a certificate on the register and its retrieval in an efficient manner. The system verifies the authenticity of the records of the certificates by the verification ID when verifying the records and comparing it with available information stored on the system. The proposed solution improves the validity, integrity, and the quality of checking digital certificates.

***Keywords*— Certificate Verification System, De-duplication, Supabase, Digital Credentials, Fraud Prevention, SDG 4 - Quality Education, SDG 9 - Industry, Innovation, and Infrastructure.**

I. INTRODUCTION

The authentication of academic certificates is an essential activity in the education system, recruitment system, as well as professional appointing systems. However, as the quantity of counterfeits and counterfeit certificates is increasing, it has introduced severe challenges to the organisational logistics of the document validation which allows for documents to documents presented. The way of manual verification is a burden that is unproductive and can be abused, just like the traditional system. In this era of digital revolution of academic and the administrative industry, the need is a safe automated certificate verification system.This paper details a cloud based Certificate Verification System which has been conceptualized to deliver the issuance of academic certificates and on-the-fly authentication.

Grenze ID: 01.GIJET.12.2.373_24

Its architecture consists of two main modules, the first one named Admin where authorized users have the right to post and update the metadata of the certificates, and the other one called Verifier that can be used in being authenticated by scanning a QR code written on the physical certificate. It is set up on the Supabase platform that provides authentication service, database administration and cloud storage facility. The certificates will offer their own version of serial number and be linked to online verification portal hence making them to be automatically authenticated. The data objects in the database provide redundancy and data integrity by using database-level unique constraints that subsequently ensure that there are no duplication or redundancy of values in the data items. The system proposed due to the cloud architecture and the use of QRs in authentication will result in a more transparent system, with fewer steps that people need to perform, will be more scalable, and will be trusted as it will provide a secure means to handle the academic qualifications. The extreme use of digital technologies in the educational and management domain has intensified the need to find secure cloud-based services, which will provide not only accessibility but also reliability. Issues related to the inefficiency in the verification of certificates are common to the employers and educational institutions, which can be explained by the time span of communications and the lack of centralized databases. An online authentication system reduces these barriers through providing instant access to verified documentation through a secured online platform.The proposed system can assist in quick validation utilizing QR code technology with the help of a cloud database so that a manual verification will not be needed anymore. This does not simply reduce the time of verification, but also enhances trust between the issuers of certificates and those that get to the receivers of the certificates. The centralized storage model provides the uniformity of certificate data maintenance and limits the unauthorized change of data by means of controlled access. Generally, the system can be used to improve the efficiency of the operations, curb fraud and transparency in operations of institutional credential checks.

II. Literature Survey

A blockchain-based (2023) verification and de-duplication framework of cloud-storage environments was proposed by V. S. Walunj, P. Gupta, and T. J. Parvat. The authors utilize smart-contract to find redundant data and expose integrity breach. [1]

By based on a fog-aid cloud network, Frederik Jakkarin Lapmoon and Somchart Fugkeaw designed a provable and safe scheme of data de-duplication designed to work within a peer setting of industrial Internet of Things (IoT) components in 2025. The architecture ensures real time integrity checking, reduces storage redundancy and hence enhances security and reliability of distributed IoT system. [2]

Ke Gu and co- authors (2024) proposed a distributed auditing and de-duplication of data on blockchain of shared information in cloud-fog computing environments relating to Vehicular Ad Hoc Network (VANETs). One of the ways that the scheme enhances data integrity, removes redundant data storage, and enhances security in vehicular communication infrastructures is its combination of blockchain and distributed audit elements. [3]

Rahul Mishra et al. (2023) suggest an opportunity to create an efficient solution to the issue of data duplication in clouds by offering a redactable blockchain-based framework that allows ensuring effective public auditing in a decentralized manner. This allows their approach to ensure controlled amendment of blockchain records without destroying transparency and therefore improve storage efficiency and audit reliability. [4]

Mingyang Song et al. (2023) propose a system of deduplication and integrity auditing of encrypted cloud storage, which uses blockchain. The system is secure in reference to duplicate detection and integrity verification of data without exposing sensitive information hence enhancing on the security as well as optimization on storage. [5]

III. Proposed Work

A ladder to a cloud-based Certificate Verification and Management framework has been introduced that would help reduce the culminating problems which are related to certificate forgery, duplication and the inefficiencies of the manual verification procedures. The overall aim is to create a safe, open-ended, and decentralized electronic platform through which institutions are able to create certificates electronically and thus allow instant authentication by valid users or third parties. The structure is designed to consist of two main elements namely an Admin Module and a Verifier Module that is linked through a centralized cloud database structure. The issue and full management of certificates is assigned to the Admin Module which handles issues of issuing certificates which are secure and protected. Certified administrators are authenticated with sound systems, only after which they add certificate details to the system. Most important attributes among the records are selected, such as serial number, name of the certificate holder, course details and date of issue. Each certificate is given a unique serial

number to ensure that it is differentiated in the database. At the same time, each certificate has a QR code created in real time, and it is a URL with a verification page, and it links directly to a validation page on the Internet. The QR code is also enclosed in the physical certificate and thus, it can be verified later by scanning. The Verifier Module eases real time validation of certificates.

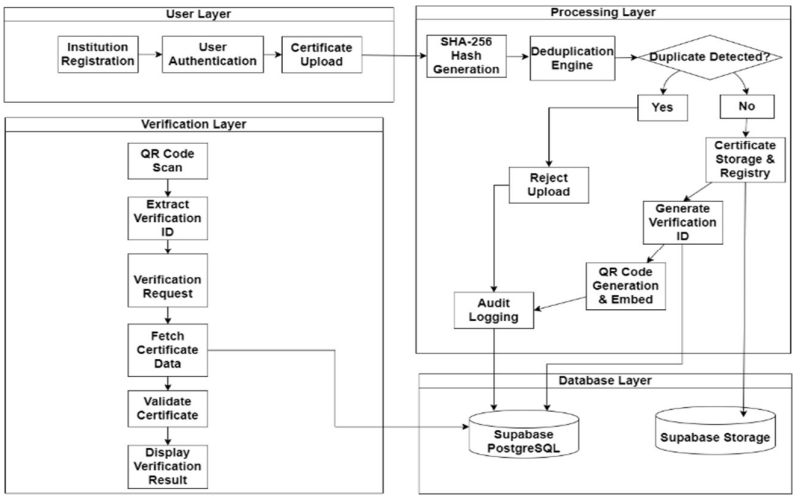

Fig. 1. Block diagram representation for proposed Methodology

IV. METHODOLOGY

A. Problem Statement

Conventional digital certificate systems, in most cases, are directly based on manual verification system and, therefore, they are susceptible to duplication, alteration, and delays in verification. In most cases, to determine whether a certificate is authentic or not, one will have to reach the issuing institution, which is very inefficient and time consuming. Also, there are no safe digital validation systems, which can further pose the threat of counterfeit or duplicate certificates being traded. To overcome these obstacles, the proposed system deploys a secure digital certificate verification system which incorporates cryptographic hashing, QR-code based validation, as well as cloud storage. The system provides the integrity of certificates, keeps off duplication in registration of certificates, and provides fast and reliable verification through an automated validation system.

B. System Architecture

Figure 1 depicts the architecture of the proposed system of verifying the digital certificate. The system adheres to the layered architecture that has four major complexes, namely User Layer, Processing Layer, Database Layer and Verification Layer. All layers have individual functions connected with the authentication, certificate validation, data storage, and certificate validation. Figure 1 demonstrates that the process of work starts when an institution communicates with the system with the help of the User Layer. The certificate that is uploaded is processed, thus, in the Processing Layer where cryptographic hashing and duplicate detection actions are taken. The deduplication engine is used to analyse the existence of certificate in a system. In case of a duplicate, the request to upload is not accepted. Otherwise, there is a generation of a verification ID and QR code. The metadata of the certificate and the files are next stored in Database Layer. The user verifies the certificate record by scanning the QR code in the certificate and this enables the system to fetch and confirm the certificate record in the database. This multi-layered architecture provides a secure certificate management, efficient verification and scalable data storage.

C. User Layer

The primary interface of the system is the User Layer which allows the institutions to interact with the system. This layer handles the institutional registration, authentication and uploading of certificates. The institutional users during the registration process provide password and email address. Supabase Authentication is applied in this system to handle the secure storage of credentials and user authentication. The system uses the bcrypt hashing algorithm to generate cryptographic hash values out of passwords instead of storing them in plaintext.

D. Processing Layer

The Processing Layer achieves the main computation processes needed to undertake certificate validation, duplicate detection, and certificate registration.

SHA-256 Hash Generation

When uploading a certificate, the system will create a SHA-256 cryptographic hash of the file certificate. SHA-256 is a variant in the SHA-2 group of hash algorithms and generates a 256 bits fixed-length hash. The hash generated in this step essentially acts as a unique fingerprint for the certificate. The reason hash is used in this step is because hash functions are known to obey the avalanche effect, wherein a small change in input will always produce a completely new hash value.

Deduplication Engine

During this step, a deduplication engine is used to match the hash generated in the previous step with those already present in the database. As illustrated in Figure 1 above, a check is performed by the deduplication engine to match the hash generated in the previous step with those already present in the system.

Verification ID Generation

For all legitimate certificates identified in this step, a unique identification code referred to as the verification ID is generated. This code essentially serves as a reference key to identify a certificate in the system for purposes of verification. The generated code ensures that a certificate is identified uniquely in the system's database.

QR Code Generation and Embedding

After generating a unique identification code referred to as a verification ID in this step, a QR code is generated with this code embedded in it. The generated QR code is then embedded in the certificate document to allow easy scanning by the certificate verifier to begin the verification process. The embedding of the generated QR code in this step ensures easy authentication of a certificate by a verifier without having to input any details to begin the verification process.

Audit Logging

To allow traceability within the system, an audit logging mechanism is integrated in this step in the system's processing layer.

Database Layer

This is where the location of the certificates is managed and how they can be accessed. In this case, the cloud is used with Supabase PostgreSQL and Supabase Storage. This is a relational database that allows us to index the certificates quickly and retrieve the relevant information as soon as the verification process is initiated. On the other hand, the certificates themselves are stored in Supabase Storage, which is a cloud-based storage solution that is designed specifically for storing digital documents. In this case, the database holds the links to the certificates.

E. Verification Layer

This is the part of the process where the user can verify the legitimacy of the certificate. This is initiated when the user uses their device to scan the QR code on the certificate. The QR code is linked to the verification ID that is used at the time of issuance. Once the scanning is initiated, the verification ID is obtained. A check is then run on the backend to retrieve the relevant information from the database based on the verification ID. Validation is then run to check whether the certificate is present in the database and whether the information matches the one that is retrieved. If the certificate is found, then it is valid. Otherwise, it is deemed invalid, which may be a forgery or the certificate is not registered.

F. Certificate Deduplication Algorithm

To process the deduplication and registration of the certificate in a simple and straightforward manner.
Input: Certificate C, which is obtained from a trusted institution after the authentication process.
Output: Result of the certificate registration process.

V. Results and Discussion

To assess the usefulness of the developed certificate verification system, it had been compared to a blockchain-based certificate verification strategy. The performance parameters to be evaluated include verification speed and storage capacity which are two significant performance parameters. The data on the characteristics of the

blockchain system behaviour was analysed based on the material in the Ethereum blockchain dataset whereas the proposed system was tested based on the record about certificates that were stored in a Supabase PostgreSQL database and cloud storage.

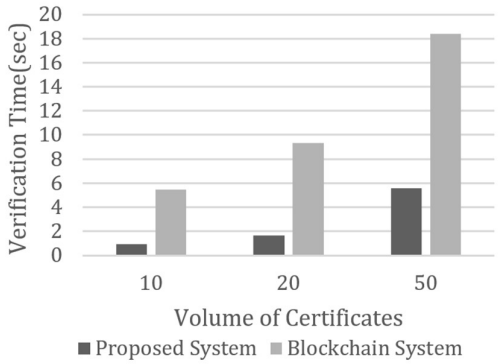

Fig. 2. comparison of Verification Speed for Block Chain System and Proposed System

Figure 2 shows the time comparison of the certificate verification in the proposed system and the blockchain based certificate verification system compared by the volume of certificate being verified. The authentication of a certificate in the wild of blockchain-based verification systems involves retrieval of transaction records that include a certificate hash on the blockchain network. This is a process which entails transaction verification, block validation, and distributed network synchronization and this raises the verification latency. Unlike, the proposed system uses direct database queries based on certificate serial numbers to verify the certificates, and this allows the fast retrieval of the certificate information. Such findings prove that the suggested system offers much faster certificate validation than the method based on the blockchain as it uses effective database queries rather than distributed ledger transaction validation.

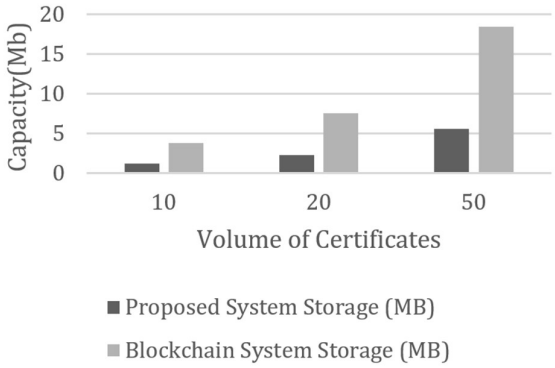

Fig. 3. comparison of Storage for Block Chain System and Proposed System

As shown in figure 3, storage requirements in the proposed system are compared to that of certificate verification system based on the blockchain with certificate volume of 10, 20 and 50 certificates. The structured data can be effectively managed and the suggested system provides a high-performing storage management and a structured data retrieval allowing the certificate metadata to be stored in a PostgreSQL and certificate documents to be stored in Supabase cloud storage. These findings suggest that the proposed system requires much lesser storage capacity than those that are blockchain-based. According to the obtained experimental data in Figures 2 and 3, the suggested certificate verification system shows high performance in terms of the speed of verification and storage efficiency. The cloud-based centralized architecture with Supabase allows retrieving certificates faster, and makes the storage utilization more efficient. Contrarily, blockchain-based systems create further burden on the computational and storage by synchronizing the distributed ledger and processing of transactions. Thus, the suggested system offers an improved, scaled-up, and sensible solution to certificate validation in the educational facilities and training companies.

VI. OUTPUT

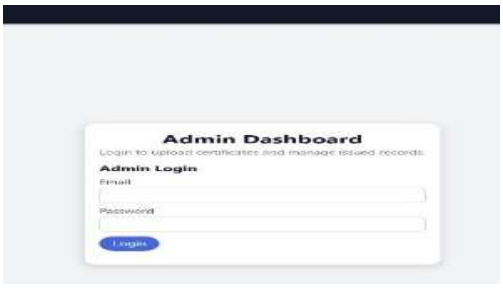

Fig. 4. Admin login interface

The proposed Certificate Verification System will contain an administrative login interface that will enable the free access of administrative dashboard, where operations will take place relating to the management of certificate. The administrator will need to provide valid login credentials such as an email address and a password that he or she will authenticate using a backend authentication service that is built on Supabase. After authentication, the system creates an authenticated user session and redirects the user to the dashboard where a user can upload certificate records and manage them. Such authentication will ensure that only authorized staff can access the certificate management module, ensuring the system is not accessed by unauthorized personnel and reducing the certificate data integrity of the data held in the cloud database.

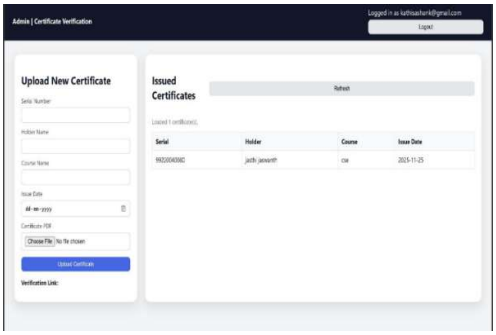

Fig. 5. Admin Certificate management dashboard

The certificate verification interface of the proposed system enables the verifier to key in the serial number of the certificate he or she is verifying or scan the QR example embedded in the certificate to start the procedures which attracts and verifies his certificate. After the request is submitted the system will query the cloud database and give the result of the verification almost in real time. In the case the certificate record is found, the system validates the certificate and uncovers the stored attributes like serial number, name of cert holder, course with which the certificate was issued and the date of issue of the certificate. In addition, the interface provides the preview of the certificate PDF uploaded, thus allowing the verifier to provide visual support to the contents of the certificate. This means that this module will make certificate authentication fast and reliable via a simple web interface.

Fig. 6. Certificate verification interface

The administrator dashboard, which is the tool to be used in managing certificate records in the proposed system will give the authorized user the ability to add new certificates by adding certificate details such as: serial number, holder name, course name, date when it is issued and a respective PDF file. Once the certificates have been uploaded, the certificate information remains at the cloud database and it is rendered in the issued certificates table.

There is also a refreshing option on the dashboard that properly displays the certificate list and a review of all issued certificates along with the metadata contained. Therefore, this module will result in a competent issuing of certificates, data storage, and ensuring a safe custody of certificate records in the system. It has proven to be effective as the addition of cloud-based storage to automated certificate validation leads to a successful verification functionality.

VII. Conclusion and Future Work

In this research, we are going to introduce a cloud-based Certificate Verification System that is to facilitate the safety, effectiveness, and reliability of academic certificate escalation. The architecture includes the use of web interface and cloud backend of Supabase and the management of certificate records, authentication, and storage provider. The proposed system will provide the administrators with the opportunity to post the information about certificates securely and utilize it to generate verification links and QR codes to every certificate being issued. It is because of these QR codes that the verifiers are able to immediately be in a position to verify the certificates by scanning, or typing in the certificate serial number in the verification interface. The process of verification has enabled the system to store data on the certificate in shared cloud database as well as retrieve the data on a real time basis on command.

The experiment results demonstrate that the framework reduces dramatically the scope of the quantity of manual screening devoted to it, gets rid of the cases of duplicate certificate records owing to the application of distinct serial numbers, and reduces the fraud of certificate scam. Accordingly, the system is a feasible, scalable and effective way of practicing the activity of validating digital certificates in the educational establishments and other companies tied with it. Although the performance offered by the proposed system is reliable, there are a number of potential avenues through which the same can be improved. The advanced cryptographic methods or blockchain may be used in the future work in order to provide the tamper-proof record of certificates and decentralized verification systems.

In addition, administrators should use multi-factor authentication, which would enhance security in the system. Future versions may also involve automatic generation of certificates, email notification on issuing the certificate, and connection with the institutional management software. This should be enhanced by the inclusion of mobile application to certify the certificates and should allow users to check certificates directly through mobile devices. All these potential improvements would increase the scalability, security and usability of the certificate verification system in live applications.

References

[1] Walunj, V.S., Gupta, P., Parvat, T.J. (2023). Verify De-Duplication Using Blockchain on Data with Smart Contract Techniques for Detecting Errors on Cloud. In: Jeena Jacob, I., Kolandapalayam Shanmugam, S., Izonin, I. (eds) Expert Clouds and Applications. ICOECA 2022. Lecture Notes in Networks and Systems, vol 673. Springer, Singapore. https://doi.org/10.1007/978-981-99-1745-7_64

[2] NICHOLAS, BISASO. "Secure Block-Based Data De-Duplication System Using Hash-Code Referencing Technology: Case Study: Backup International Uganda (Doctoral Dissertation." Uganda Martyrs University (2016)

[3] Zhang, Guipeng, et al. "A secure authorized deduplication scheme for cloud data based on blockchain." Information Processing & Management 58.3 (2021): 102510.

[4] Lapmoon, Jakkarin, and Somchart Fugkeaw. "A verifiable and secure industrial IoT data deduplication scheme with real-time data integrity checking in fog-assisted cloud environments." IEEE Access 13 (2025): 11969-11988.

[5] Gu, Ke, et al. "Blockchain-based data deduplication and distributed audit for shared data in cloud-fog computing-based vanets." IEEE Transactions on Network and Service Management 21.5 (2024): 5548-5565.

[6] Mishra, Rahul, et al. "Enabling efficient deduplication and secure decentralized public auditing for cloud storage: A redactable blockchain approach." ACM Transactions on Management Information Systems 14.3 (2023): 1-35.

[7] Song, Mingyang, et al. "Blockchain-based deduplication and integrity auditing over encrypted cloud storage." IEEE Transactions on Dependable and Secure Computing 20.6 (2023): 4928-4945.

[8] Zhang, Guipeng, Pinghua Chen, and Yongwei Liao. "Blockchain-based secure and verifiable deduplication scheme for cloud-assisted internet of things." IEEE Internet of Things Journal 11.8 (2023): 13995-14006.

[9] Li, Shanshan, et al. "Blockchain-based transparent integrity auditing and encrypted deduplication for cloud storage." IEEE Transactions on Services Computing 16.1 (2022): 134-146.
[10] P. Sathyabama, M. Shalini, R. Dhivya Bharathi, G. Sathi, K. Thilagam and S. Uma Maheswari, "Ensuring Confidentiality: A Secure Deduplication Model to Prevent Healthcare Records over Cloud Computing Environment with Advanced Crypto Logics," 2024 4th International Conference on Intelligent Technologies (CONIT), Bangalore, India, 2024, pp. 1-7, doi: 10.1109/CONIT61985.2024.10626955.
[11] Periasamy, J. K., et al. "Enhancing cloud security and deduplication efficiency with SALIGP and cryptographic authentication." Scientific Reports 15.1 (2025): 30112