



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Student Document Attestation System

Dr. Rajini S, Manoj P Kumar, Ammogh Ashok, Meghanashri V, Aditya Prakash

Department of Information Science and Engineering, Vidyavardhaka College of Engineering, Mysore, India

ABSTRACT: With an estimated 26 million students enrolled in Indian higher education and nearly 10 million graduates annually, every student, whether in high school or graduating, needs to validate all their records from school to college and beyond. From undergraduate to postgraduate and all the degrees, diplomas and transcripts in between, the current system requires students to get their documents attested by government officials of the respective city. This is a cumbersome process that can take time and effort. This is why it is important to ensure all records are reliable, valid and up-to-date to ensure your educational journey is smooth and settled. This might lead to document lose, document forgery. To make this process safe and secure everything can be digitized with the theory of confidentiality, availability and Reliability. All of this can be achieved by using AES Encryption and Secure storage using AWS S3 storage. This method involves the student uploading his documents to the storage by encrypting his documents by AES encryption which is one of the most secure algorithms that exists in the current generation. These documents will be validated by panel members those are officials who work for the government in various departments such as Medical, Police force, Education department. The use of a digital certificate system provides students with numerous benefits. Not only does it reduce the risk of losing or damaging a physical certificate, but it also allows for quick and efficient validation of the certificate. By foregoing traditional paper certificates, the student is able to access and verify their credentials in a secure and streamlined manner.

KEYWORDS: Digital Certificate, AES Encryption, Certificates Creation and Authentication, AWS S3 storage.

I. INTRODUCTION

The validation and security of educational documents play a pivotal part in a pupil's academic trip and professional career. In India, like numerous other countries, scholars face multitudinous challenges related to the verification and protection of their educational credentials. These challenges include the threat of document loss, damage, and phony, which can have severe counteraccusations when applying for advanced education, employment, or other professional openings. Addressing these challenges is of utmost significance to insure a dependable and effective system that benefits both scholars and institutions. In the current system, educational documents are generally stored and changed in physical form, similar as paper instruments and mark wastes. still, this traditional approach presents several limitations. Physical documents are vulnerable to colorful pitfalls, including loss due to mishandling or accidents, damage caused by natural disasters or deterioration over time, and unauthorized duplication or revision. These pitfalls not only vexationscholars but also undermine the credibility and integrity of the entire education system. To overcome these challenges, there's a growing need to embrace technological advancements and explore digital results for the confirmation and security of educational documents. By digitizing the document verification process, we can alleviate the pitfalls associated with physical documents and streamline the confirmation process, making it more effective and dependable. The ideal of this study is to propose a secure and robust system that leverages technology to address the challenges faced by scholars in India regarding the confirmation and security of their educational documents. The proposed system aims to give a secure platform for scholars to store their documents digitally, icing their confidentiality, integrity, and availability. also, it seeks to establish effective mechanisms for the confirmation of these documents by applicable authorities and stakeholders. One of the crucial factors of the proposed system is the use of Advanced Encryption Standard(AES) encryption and secure storehouse through Amazon Web Services(AWS) S3. AES encryption ensures that the documents are defended from unauthorized access and tampering, while AWS S3 provides a largely secure and dependable pall storehouse structure for storing the translated data. This combination of encryption and secure storehouse ensures the confidentiality and integrity of the documents throughout their lifecycle. also, the proposed system incorporates the involvement of government officers from colorful departments in the confirmation process. These officers would be granted secure access to the translated documents and would corroborate the information handed by the scholars. The use of digital instruments plays a vital part in this process, enabling effective confirmation and reducing the reliance on physical documents. To develop the proposed system, a comprehensive review of being literature on analogous systems is conducted. This review explores the use of blockchain technology, two- factor authentication, digital autographs, and AWS S3 storehouse in securing educational documents. The advantages and disadvantages of these styles are anatomized, considering factors similar as trust, rigidity, and

comprehensive security measures. By enforcing the proposed system, scholars would witness a significant enhancement in the availability, security, and confirmation of their educational documents. The digitization of documents would reduce the pitfalls associated with physical clones, similar as loss or damage, while the secure storehouse and encryption would insure the confidentiality and integrity of the data. also, the involvement of government officers and the use of digital instruments would enhance the confirmation process, making it more effective and dependable for all stakeholders.

II. BACKGROUND AND RELATED STUDY

2.1. AES Encryption

AES(Advanced Encryption Standard) encryption is employed in the Student Data Attestation CS Engineering design to insure the security and confidentiality of sensitive pupil information. AES- 256, a extensively espoused encryption algorithm, is employed in the design, using a 256- bit encryption key. With AES encryption, pupil data similar as particular information, academic records, and documentation documents are translated before being stored in the design's database or transmitted over the network. This encryption process makes the data ungraspable to unauthorized individualities, furnishing an fresh subcaste of protection against unauthorized access. To further enhance security, the design tools secure crucial generation and operation practices. Strong encryption keys are generated and securely stored, with limited access only granted to authorized labor force. Regular crucial gyration is also employed to minimize the threat of crucial concession. When transmitting pupil data over the network, secure communication protocols like SSL/ TLS are employed to establish an translated connection. This ensures that the data remains defended during conveyance,securing its integrity and confidentiality. The design's database system is designed with robust security measures, including access controls and authentication mechanisms. Unauthorized access attempts are laboriously covered, and applicable measures are in place to help unauthorized manipulation or reclamation of the translated data. Added to it, the project tools user authentication mechanisms analogous as strong passwords andmulti-factor authentication to control access to the system. This ensures that only authorized labor force can pierce and work with the pupil data. Regular security checkups and vulnerability assessments are conducted to identify and address any implicit sins in the AES encryption perpetration. Software updates and patches are instantly applied to maintain a high position of security and cover against arising pitfalls. By incorporating AES encryption into the Student Data Attestation CS Engineering design, the end is to prioritize the security and sequestration of pupil information. AES encryption, along with secure crucial operation, data transmission, and access control measures, helps maintain the confidentiality, integrity, and vacuity of the data throughout the documentation process.

2.2.Two Factor Authentication

Two-factor authentication (2FA) is implemented in the project to improve the security of user access and secure sensitive information. It adds an extra layer of verification beyond traditional username and password authentication.

With 2FA, users are required to provide two types of authentication factors to gain access to the system. These factors typically fall into three categories:

Knowledge Factor: This factor involves something the user knows, such as a password or PIN. Users are required to provide a correct password during login.

Possession Factor: Users receive a unique one-time verification code through an email

To complete the login process with 2FA, users must provide the correct password (knowledge factor) and enter the verification code from their email (possession factor). This additional step ensures that even if an unauthorized person obtains or guesses the password, they would still have to access to the user's email to complete the authentication process.

By implementing 2FA, the project strengthens the security of user accounts and mitigates the risk of unauthorized access. It adds an extra layer of protection against password theft, brute-force attacks, and phishing attempts, significantly reducing the likelihood of unauthorized access to sensitive student data.

It is important to choose a secure and reliable 2FA method and educate users about its benefits and proper usage to ensure the successful implementation and adoption of this additional security measure.

2.3.AWS S3 Storage

AWS S3 (Amazon Simple Storage Service) is a veryreliable and secure cloud storage solution that can be leveraged in our student certificate validation system. With AWS S3, we can efficiently store and manage the certificates uploaded by students, facilitate access for validators to download and validate the certificates, and allow students to retrieve the validated certificates.

Storage and Uploading: AWS S3 provides a reliable and durable storage infrastructure to store the certificates uploaded by students. When a student uploads their certificate, it can be securely stored in an S3 bucket. S3 supports various uploading mechanisms, including API integration or direct file uploads via web forms.

Access Control: AWS S3 offers flexible access control mechanisms to ensure that only authorized validators and students can access the stored certificates. Access permissions can be configured at the bucket level or for specific objects within the bucket. Validators are granted read access to download and validate the certificates, while students have read access to retrieve their validated certificates.

Validator Download and Validation: Validators with appropriate access credentials can download the certificates from the S3 bucket for validation. The downloaded certificate can be processed using the validation logic specific to our system. Validators can perform the necessary checks, verify the authenticity of the certificate, and ensure its compliance with the required standards.

Uploading Validated Certificates: Once the certificate is validated, validators can upload the validated certificate back to the AWS S3 bucket. This ensures a centralized repository of validated certificates, making it easy to retrieve and distribute the certificates to the respective students.

Student Access and Retrieval: After the certificate is successfully validated and uploaded to the S3 bucket, students can securely access and retrieve their validated certificates. Students can download their certificates from the S3 bucket using appropriate authentication mechanisms or web interfaces provided by our system.

Security and Scalability: AWS S3 offers robust security features, including encryption at rest and in transit, to protect the confidentiality and integrity of the stored certificates. Additionally, AWS S3 is highly scalable, allowing us to accommodate a growing number of certificates and users without compromising performance.

By leveraging AWS S3 storage in our student certificate validation system, we ensure secure and efficient storage of certificates, streamlined access for validators to download and validate certificates, and easy retrieval of validated certificates by students. The scalable nature and comprehensive security features of AWS S3 contribute to the reliability and integrity of our certificate validation process.

2.4.Digital Signature

A digital signature is a cryptographic technique used to verify the authenticity, integrity, and non-repudiation of electronic documents. In the context of the certificate attestation process, a digital signature is employed to ensure the validation and integrity of the certificate.

When the student uploads their certificate, the validator can download it from the system. The validator then verifies the contents of the certificate, ensuring its accuracy and compliance with the required standards. After confirming the validity of the certificate, the validator digitally signs it.

The digital signature is generated using the validator's private key, which is securely stored and uniquely associated with them. This private key is used to encrypt a hash value generated from the certificate. The encrypted hash value serves as the digital signature. It uniquely identifies the validator and provides evidence that the certificate has been attested by them.

Additionally, the validator may add their stamp or seal to the certificate to further signify its attestation. This stamp can be a visual representation of their authority or organization.

Once the certificate is digitally signed and stamped, the validator uploads it back to the system. This completes the attestation process and ensures that the certificate remains tamper-proof. The digitally signed certificate and the validator's stamp serve as proof of the validation and attestation by an authorized entity.

The digital signature provides several benefits in this process. Firstly, it ensures the integrity of the certificate, as any modifications or tampering would invalidate the signature. Secondly, it verifies the authenticity of the validator, as the digital signature can only be generated with their unique private key. Lastly, the non-repudiation aspect prevents the validator from denying their attestation, as the digital signature acts as irrefutable proof.

By employing digital signatures, the certificate attestation process becomes more secure, trustworthy, and efficient. It enables the validation of certificates by authorized validators, adds a layer of integrity and authenticity, and provides a reliable method to track and verify the attestation process.

2.5.Cloud Storage

Cloud storage is utilized in our system to store various data related to students, validators, and exam centers. This cloud-based storage solution securely stores information such as user names, addresses, localities, and other relevant details, excluding the certificates themselves. The certificates, however, are specifically uploaded and stored exclusively in the AWS S3 storage.

Cloud storage offers several advantages for our system:

Data Centralization: Storing student, validator, and exam center data in a centralized cloud storage allows for easy access, management, and retrieval of information. It eliminates the need for physical storage and enables efficient organization of data.

Scalability and Flexibility: Cloud storage can dynamically scale to accommodate growing amounts of data without requiring additional infrastructure. It offers the flexibility to adapt to changing storage needs, ensuring that our system can scale as the number of users and data increases.

Data Security: Cloud storage providers implement robust security measures to protect stored data. This includes encryption at rest and in transit, access controls, and regular security updates. These security features help safeguard sensitive information and mitigate the risk of unauthorized access or data breaches.

By utilizing cloud storage for student, validator, and exam center data, we ensure a secure, scalable, and efficient storage solution. The separation of certificate storage to AWS S3 provides an additional layer of security, as it is specifically designed for the secure storage and retrieval of sensitive documents like certificates.

2.6 Problem Statement

The process of document attestation is a crucial aspect of international travel and migration. It involves verifying the authenticity of various documents, such as educational certificates, birth certificates, and marriage certificates. However, the current document attestation system is often time-consuming, cumbersome, and prone to errors. This can cause significant delays and inconvenience for individuals and organizations that need to get their documents attested.

Moreover, the current system is also susceptible to fraud and corruption. There have been instances where forged documents have been attested, leading to serious consequences for individuals and organizations. In addition, the traditional attestation process involves physical copies of documents being sent to various authorities, which can be lost, damaged or delayed in transit.

Therefore, there is a pressing need for a more efficient, secure and reliable document attestation system that can reduce the time and effort required to get documents attested, while also ensuring the authenticity of the documents. The system should also be able to prevent fraud and corruption, and provide a seamless and streamlined attestation process for individuals and organizations.

III. METHODOLOGY

3.1 Application Manager

The Application Manager module manages all other modules: Student, Validator, and Exam Centre.

It handles the integration, coordination, and communication between the modules.

The Application Manager also creates the Exam Centre login for managing exam-related functionalities.

3.2 Student Module

Students register and create profiles in the Student module.

They upload their certificates to the system for validation.

Students can select a Validator from their locality who is currently online.

3.3 Validator Module

Validators register and create profiles in the Validator module.

The Validator can view the list of validation requests from students in their locality.

The Validator can access and download the certificate uploaded by the student from AWS S3 storage, ensuring that it is accessible only to them.

After reviewing the document, the Validator attests it if it meets the required criteria.

The Validator uploads the attested certificate back to the system.

3.4 Exam Centre Module

The Application Manager creates a login for the Exam Centre module.

The Exam Centre can add exams to the system, including exam details and requirements.

Students can apply for exams through their Student module login.

The Application Manager facilitates communication between the Exam Centre and other modules

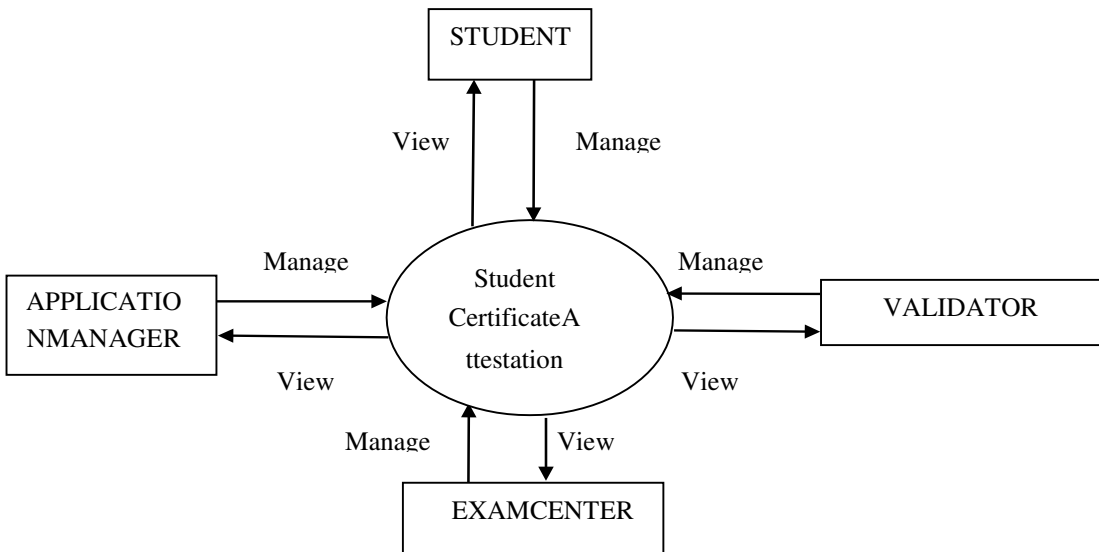
3.5 Student Application to Exam

Students, upon logging into their Student module account, can browse and apply for exams added by the Exam Centre. They provide the necessary details and can choose to attach their validated certificate obtained through the document attestation process.

The Exam Centre receives the application details and the validated certificate for further processing.

3.6 Exam Centre Verification

The Exam Centre module verifies the eligibility and authenticity of the student's application and the attached validated



certificate.

The Exam Centre cross-checks the certificate with the required documents for the exam.

Figure 1 data flow diagram of all modules

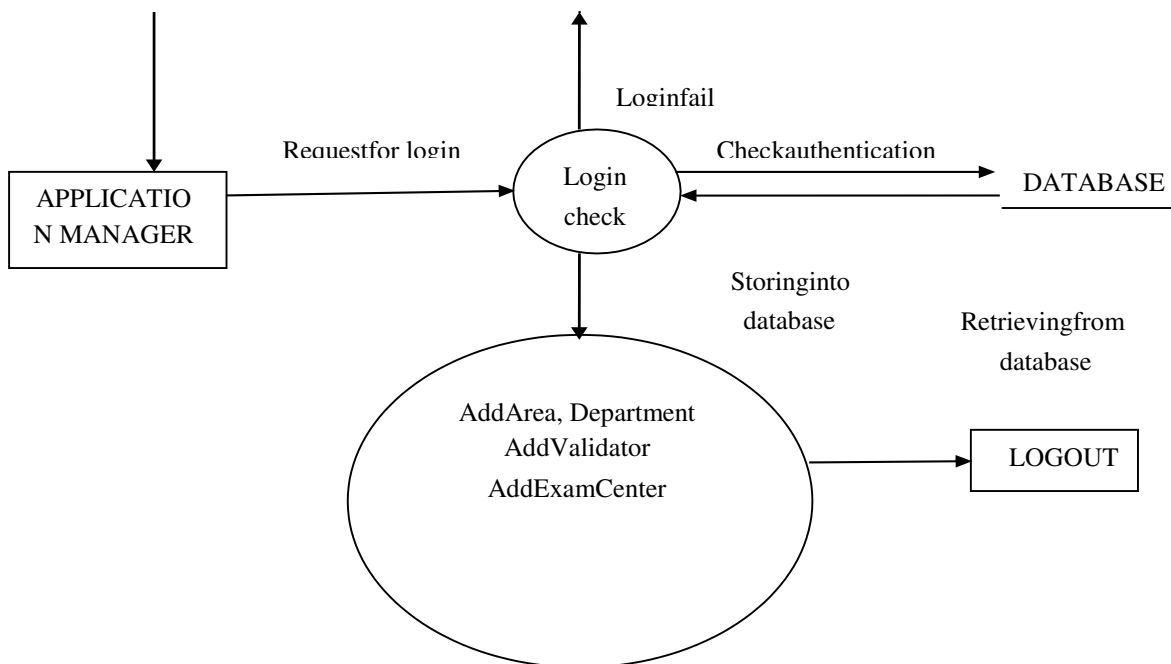


FIGURE 2 DATA FLOW DIAGRAM OF APPLICATIONMANAGER

IV. CONCLUSION

In conclusion, this survey paper has explored the concept of student data attestation and its implications in various educational contexts. Through an in-depth analysis of the student data attestation project, we have gained valuable insights into its methodology, benefits, and challenges.

The survey began by highlighting the significance of student data attestation in ensuring the authenticity and integrity of educational records. We discussed the necessity of implementing a secure and efficient system that allows students to validate their documents while maintaining data privacy.

Throughout the paper, we examined the key components of the student data attestation project, including the modules of student, validator, exam center, and application manager. We discussed how these modules interact with each other under the management of the application manager, creating a streamlined process for document validation.

The survey also shed light on the technological aspects of the project, such as the utilization of AWS S3 storage for secure document storage and access. We emphasized the importance of maintaining strict access controls to ensure that only the authorized validator can retrieve and attest the uploaded certificates.

Conflict of interest

The corresponding author declares that there are no competing interests on behalf of the other writers.

REFERENCES

- [1] Certificate Verification using Blockchain and Generation of Transcript Authors Ravi Singh Lamkoti , Devdoot Maji , Hitesh Shetty Journal, Year Vol. 10 Issue 03, March-2021
- [2] Secure Sign: Signing Document Online Authors Al Anood K. Alzahrani, Malak K. Alfosail, Maryam M. Aldossary, Muneera M. Almuhaideb, Sarah T. AlqahtaniNazar A. Saqib, Khalid A. Alissa, Norah A. Almubairik Journal, Year 2018 , IEEE
- [3] DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents Authors IftekherToufique Imam, Yamin Arafat, Kazi Saeed Alam and Shaikh AkibShahriyar Journal, Year Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2021)
- [4] Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code Authors Muhammad Umar Abdullahi , Dr. G. I.O. Aimufua, and Adamu Aminu Muhammad Journal, Year IOSR Journal of Computer Engineering (IOSR-JCE) 2022.
- [5] International Journal of Computer Science and Mobile Computing :TWO FACTOR AUTHENTICATION Authors Asif Amin , Israr ul Haq , Monisa Nazir Journal, Year July 2017
- [6] A survey of TWO FACTOR AUTHENTICATION Methods : Advantages & Disadvantages Authors ShiburajPappu, DhanashreeKangane, Junaid Mandwiwala Journal, Year JETIR, 2021
- [7] Two Factor Authentication Made Easy Authors Alex Q. Chen, Weihan Goh Journal, Year June 2015
- [8] Multi-Factor Authentication on Cloud Authors Salman H. Khan, M. Ali Akbar Journal, Year October 2016



INNO  **SPACE**
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379



ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 **9940 572 462**  **6381 907 438**  **ijircce@gmail.com**



www.ijircce.com

Scan to save the contact details