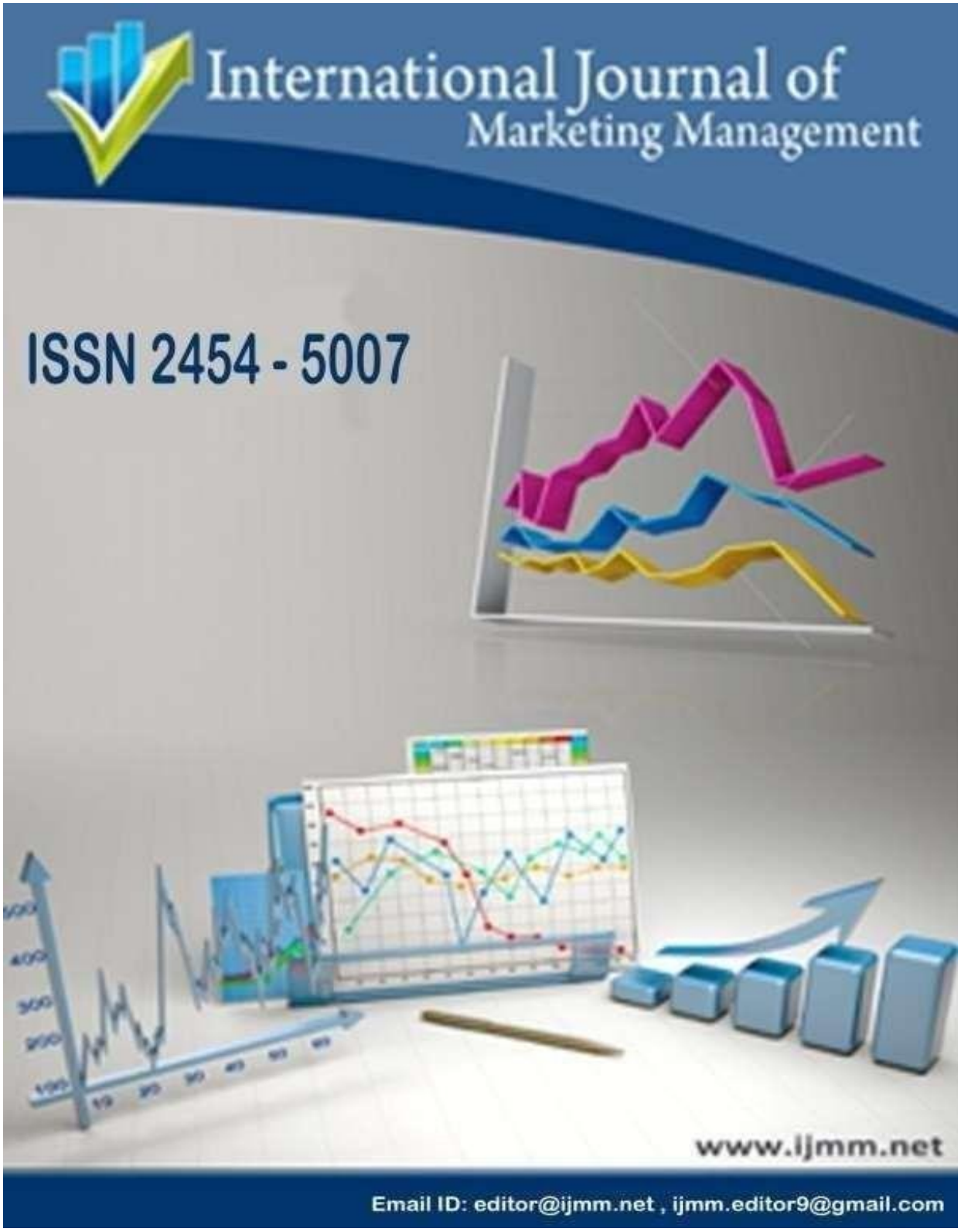
ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025



International Journal of Marketing Management

ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025

# CERTIFICATE VERIFICATION SYSTEM USING CLOUD FUNCTION AND DATABASE

**[1]Pittu Bindu Siva Madhavi, [2]Pallam Yestheru Rani, [3]Pallapu Prasanth,**

**[4]Mr. N. Lakshmi Narayana**

[1,2,3]U. G Student, Dept COMPUTER SCIENCE AND ENGINEERING, St.Ann's College Of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India
[4]Associate professor, COMPUTER SCIENCE AND ENGINEERING, St.Ann's College Of Engineering and Technology, Nayunipalli (V), Vetapalem (M), Chirala, Bapatla Dist, Andhra Pradesh – 523187, India

## *ABSTRACT*

*This project presents a cloud-based system for verifying professional and educational credentials in a safe and effective manner. It stores certificate records in a cloud database and processes data using cloud functionalities. Every certificate is given a unique ID and connected to a verification URL or QR code for instantaneous authentication. When users start the verification process, the cloud function gets the data and checks it, showing if the certificate is valid, expired, or invalid. Low maintenance, scalability, and dependability are guaranteed by the serverless design. Data integrity is protected by role-based access constraints, which restrict record updates to authorized issuers. In addition to preventing certificate forgeries and improving transparency, this system provides an affordable, internationally available verification solution.*

***KEYWORDS*** *Certificate Verification System, Cloud Function, Cloud Database, Serverless Computing, Real-time Verification, Digital Certificate Security, Data Integrity*

## INTRODUCTION

The issuing and verification of certificates have moved from conventional paper-based formats to electronic records in the current digital era. Numerous industries, including education, professional training, skill development, and compliance of the certifications, heavily rely on certificates. The shift to digital documentation has made it easier to obtain and more convenient, but it has also made it more vulnerable to illegal changes, duplication, and falsification. Because of these difficulties, it is imperative to put in place a reliable and secure system for confirming the legitimacy of certificates. These issues are addressed by the Certificate Verification System using Cloud Function and Database, which makes it possible to verify certificates securely, accurately, and in real time online. The system uses a serverless cloud function to process verification requests and keeps all certificate information in a secure database. The cloud function retrieves the relevant record from the database, verifies its authenticity, and shows the outcome immediately when a user input a certificate

International Journal of Marketing Management

ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025

ID or scans a QR code written on the certificate.

## LITERATURE REVIEW

Several research papers have explored secure certificate verification using technologies like blockchain, QR codes, and digital signatures. Studies such as those by Rahman et al. and Gangwar & Chaurasia proposed blockchain-based systems that ensure immutability and transparency but face drawbacks like high operational costs, slower transaction times, and complex implementation. Mayowa et al. introduced a QR code and AES encryption method for fast verification; however, it lacks scalability and relies on manual database management. Wellem et al. used ECDSA-based authentication for document validation, which offers strong security but increases computational overhead and deployment difficulty. In contrast, the proposed Certificate Verification System using Cloud Function and Database provides a more practical, cost-efficient, and scalable solution. It eliminates server management through serverless architecture, ensures real-time verification, and secures data with strict access control.

## RELATED WORK

Various studies have focused on creating secure and efficient certificate verification mechanisms using emerging digital technologies. Early systems relied on centralized databases and manual validation, which were time-consuming and prone to forgery. Later, researchers introduced QR code and encryption-based verification to simplify access and improve accuracy, but these systems lacked scalability and required frequent maintenance. Blockchain-based approaches were then proposed to ensure data immutability and transparency; however, they involved high implementation costs, slower response times, and complex integration. Some works also explored hybrid models combining cryptographic hashes and cloud databases, but they still required manual server management. In contrast, the proposed Certificate Verification System using Cloud Function and Database eliminates such drawbacks by adopting a serverless, cloud-driven architecture.

## EXISTING METHOD

In earlier systems, certificate verification was typically handled through manual or semi-digital processes. Most institutions relied on physical records or local databases to store and validate certificates, requiring users to contact the issuing authority directly for confirmation. Some online verification platforms used static web forms linked to institution databases, but they lacked automation, scalability, and real-time validation. Related works have proposed methods such as hash-based verification and QR code integration, where certificate data is compared using stored hash values. However, these approaches often depended on centralized servers, increasing maintenance effort and cost. Other researchers introduced blockchain-based verification systems to enhance security and immutability, but such solutions can be complex and expensive to implement for small organizations. Overall, existing systems struggle with issues of data tampering, limited accessibility, manual intervention, and lack of integration across institutions.

International Journal of Marketing Management

ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025

## PROPOSED METHOD

The proposed system advances beyond traditional verification technologies by integrating modern cloud-based and serverless computing techniques. While the existing methods depend on local servers or manual verification tools, the new system employs Cloud Functions for automated, event-driven processing without dedicated infrastructure. Certificate records are maintained in a cloud database such as Firebase Firestore, ensuring scalability, security, and real-time access from anywhere. The inclusion of QR code technology enables instant verification by simply scanning, removing the need for manual data entry. Additionally, cryptographic hashing and secure APIs are used to protect data integrity and prevent forgery. The role-based access control mechanism ensures that only authorized issuers can modify or add records. By leveraging these advanced cloud and security technologies, the proposed system offers a faster, safer, and more cost-effective verification solution compared to existing approaches.

## SYSTEM ACRHITECTURE

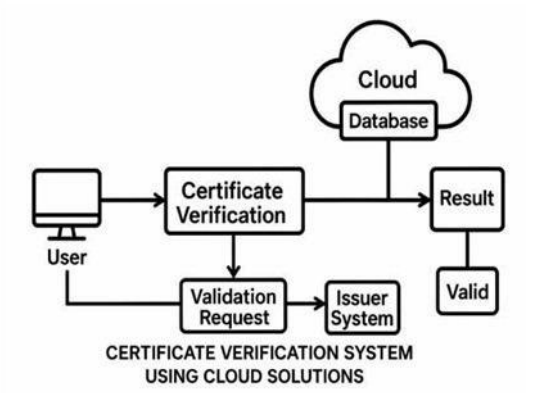



**Figure.1: System Architecture**

## METHODOLOGY DESCRIPTION

The proposed system follows a structured methodology that integrates cloud computing and database technologies for secure certificate management and verification. The process begins with the certificate issuance phase, where authorized issuers input certificate details through a web interface. The system then generates a unique ID and a cryptographic hash for each certificate, which is stored in the cloud database.

A QR code linked to the verification URL is also created and printed on the certificate. When a user scans the QR code or enters the certificate ID, a cloud function is triggered to retrieve the relevant data from the database. The cloud function compares the stored hash with the current record to confirm authenticity.

Based on the result, the system displays whether the certificate is valid, expired, or invalid. All verification activities are logged in the database for future auditing. The serverless architecture ensures scalability, low maintenance, and real-time processing. Role-based access control restricts modification privileges to verified issuers, enhancing data security and integrity.

## RESULTS AND DISCUSSION

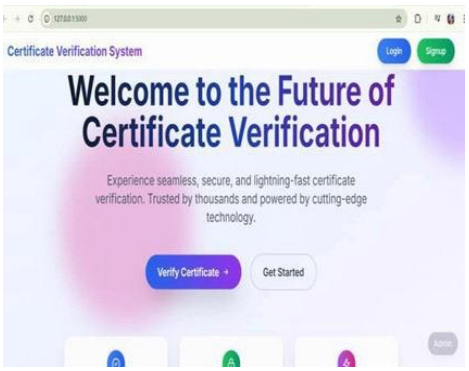



**Figure.2: Home Page**

International Journal of Marketing Management

ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025

**Home Page –** Displays the landing page with options for login, signup, and exploring feature.

**Valid Certificate Verification**

This interface allows users to upload a PNG certificate and verify its authenticity. When the user clicks Verify Certificate the system checks the uploaded file's hash with the cloud database to confirm if it is valid or tampered. It provides a quick and secure verification process through an easy-to-use web form.

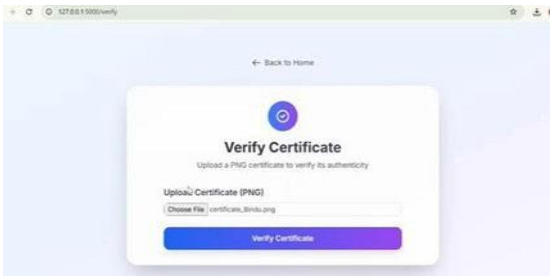



**Figure.3: The process of uploading file**

After the user clicks Verify Certificate , the cloud function retrieves the stored data from the database, matches the certificate hash, and validates its authenticity. The message "Certificate Verified! This certificate is valid and issued to Bindu for the course AI indicates that the certificate is genuine, belongs to the specified user, and has not been tampered with.


**Figure.4: Certificate Verification valid Certificate**

In this case, the verification failed because the uploaded file did not contain the necessary information. The error message states: This image does not contain a certificate hash. Please upload a valid certificate generated by this system.

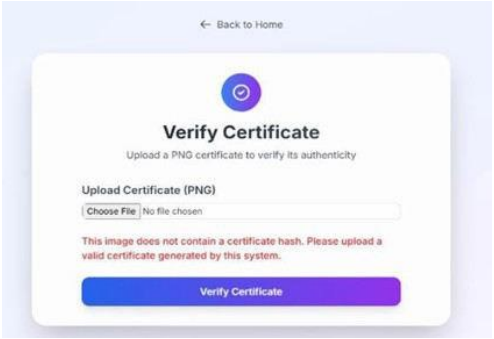



**Figure 5: Invalid Certificate Validation**

## CONCLUSION

The project provides a secure and scalable platform for issuing and verifying certificates using cloud technology. It ensures authenticity, reliability, and efficiency, laying a strong foundation for future enhancements like blockchain and mobile integration

## FUTURE SCOPE

The system has wide future enhancement, including integrating blockchain, AI, and mobile apps to enhance security and accessibility. These advancements will make the platform more intelligent, user-friendly, and globally reliable for certificate verification.

## REFERENCES

1. Harini, D. P. (2013). Scalable and Secure Sharing of Client Medical Records in Cloud. IJCST.
2. Kumutha, K. & Jayalakshmi, S. (2021). *The Impact of the Blockchain on*

International Journal of Marketing Management

ISSN 2454 5007,
www.ijmm.in
Vol. 13 Issue. 4, 2025

*Academic Certificate Verification System – Review.* EAI Endorsed Transactions on Energy Web, 8(36).

3. Gangwar, S., & Chaurasia, A. (2024). *Blockchain-Based Authentication and Verification System for Academic Certificate Using QR Code and Decentralized Applications.* International Journal of Computer Applications, 186(26), 1-10.
4. Charitha, T. S. & Baba, K. A. (2022). *A System for Academic Certificates Verification Using Blockchain.* IJRASET.
5. Naik, S. P., Patel, M. D., Limbhore, M. D., Chamriya, M., & Patil, M. (2023). *CERTI-BLOCK: A Blockchain Technology Based Certificate Validation System.* IJRASET.
6. Peyyala, J. (2022). *A Survey on Blockchain Based Documentation Verification.* IJRASET.
7. Kumar, V. & Raj, A. (2018). *CertLedger: A New PKI Model with Certificate Transparency based on Blockchain.* arXiv preprint.
8. Amanullah, M., Mishra, V. P., Mayavan, L., Tannady, H., & Kulkarni, N. (2023). *An Effective Double Verification-Based Method for Certifying Information Safety in Cloud Computing.* IJISAE.
9. Kumar, V., Kaur, T. (2022). *Cloud Functions and Serverless Computing.* IJRASET.
10. X. G., G. B., R. L., & W. Q. (2022). *Certificateless Data Integrity Auditing in Cloud Storage with a Designated Verifier and User Privacy Preservation.* Electronics, 11(23).
11. Sravanthi, K., & Sekhar, P. C. (2023). *An Efficient Integrity Verification Based Multi-User Cloud Access Control Framework using Blockchain on EHR Database.* IJISAE.
12. [Author Unknown]. (2025). *Secure and efficient ownership verification for deduplicated cloud computing systems.* Journal of Cloud Computing, 14, 20.
13. [Various Authors]. *Digital Certificate Verification Scheme for Smart Grid using Fog Computing (FONICA).* Sustainability, 13(5), 2549.
14. [Author Unknown]. *Authentication Protocol for Cloud Databases Using Blockchain Mechanism.* Sensors, 19(20), 4444.
15. [Author Unknown]. *Blockchain based certificate validation system.* International Journal of Innovative Science and Research Technology (IJISRT). ijisrt.com
16. [Open Source Project]. GitHub – *Blockchain-Certificate-Verification-System.* (source code repository) GitHub