IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15654

Cloud-based secure payment system with OTP and encrypted data storage

DINESH T[1], GOKUL S[2], KILLIVALAVAN S[3], AMARNATH J[4],

Mrs. L. SHAKIRA BANU, M.E.,[5]

Final Year Student, Aritificial Intelligence And Data Science,Dhanalakshmi Srinivasan Engineering College,

Perambalur, Tamil Nadu[1-4]

Assistant Professor,Department of Artificial Intelligence & Data Science,

Dhanalakshmi Srinivasan Engineering College(A), Perambalur[5]

Abstract: The rapid growth of digital payment systems and e-commerce platforms has significantly increased the volume of online financial transactions. However, this growth has also led to a rise in cybercrimes such as phishing, OTP fraud, and unauthorized access to sensitive financial data. Traditional payment systems lack adaptive security mechanisms, making them vulnerable to evolving fraud techniques.

This project proposes a cloud-based secure payment system that integrates OTP authentication and encrypted data storage to enhance transaction security. The system ensures that every transaction is verified through a one-time password and simultaneously sends detailed transaction information to the user's registered email. A security link is also provided to report fraudulent activities instantly to cybercrime authorities.

The proposed system focuses on protecting user data, preventing OTP misuse, and ensuring secure communication through encryption techniques. By leveraging cloud technology, the system provides scalability, real-time monitoring, and improved reliability. Overall, the system enhances security in digital payments, reduces fraud risks, and increases user trust in online transactions.

Keywords: Secure payment system, OTP authentication, Cloud computing, Data encryption, Fraud detection

I.INTRODUCTION

In recent years, online payment systems have become an integral part of daily life, enabling users to perform financial transactions easily through the internet. Services such as online shopping, internet banking, and UPI transactions have increased convenience but also introduced serious security challenges. Cybercriminals exploit vulnerabilities in these systems to steal sensitive information such as credit card details and OTPs.

One of the most common threats in digital payments is OTP-based fraud, where attackers manipulate users through phishing calls or messages to obtain OTPs and perform unauthorized transactions. Traditional systems rely only on OTP verification, which is not sufficient to prevent such attacks.

To overcome these issues, a secure system is required that not only verifies transactions but also alerts users and provides mechanisms to report fraud. This project introduces a cloud-based secure payment system with OTP verification, email confirmation, and encrypted data storage to ensure safe and reliable transactions.

II.RELATED WORK

[1]. de Oliveira N. R., Pisa P. S., Lopez M. A., de Medeiros D. S. V., and Mattos D. M. F., (2021).”Identifying fake news on social networks based on natural language processing: Trends and challenges",Information, vol. 12, no. 1, pp. 38.

[2]. Vijay J. A., Basha H. A. and Nehru J. A. (2021). “A dynamic approach for detecting the fake news using random forest classifier and NLP”, in Computational Methods and Data Engineering. Springer, pp. 331-341.

[3]. Nikiforos M. N., Vergis S., A. Stylidou A., Augoustis A., Kermanidis, K. L and Maragoudakis, M. (2020). “Fake news detection regarding the Hong Kong events from tweets", in Proc. Int. Conf. Artif. Intell. Appl. Innov. Greece: Springer, pp. 177-186.

DOI: 10.17148/IJARCCE.2026.15654

[4]. Kumar S., Asthana, R. Upadhyay S., Upreti, N. and Akbar M., "Fake news detection using deep learning models: A novel approach", (2020). Trans. Emerg. Telecommun. Technol., vol. 31, no. 2, p. e3767.

[5]. Sansonetti G., Gasparetti F., D'Aniello G., and Micarelli A. (2020. "Unreliable users detectionn in social media: Deep learning techniques for automatic detection", IEEE Access, vol. 8, pp. 213154-213167.

[6]. Ochoa I. S., Mello G. D.,Silva L. A, Gomes A. J., Fernandes A. M. R., and Leithardt, ``FakeChain V. R. Q. (2019). "A blockchain architecture to ensure trustin social media networks" in Proc. Int. Conf. Qual. Inf. Commun. Technol.Algarve, Portugal: Springer, pp. 105-118.

[7]. Shae Z. and Tsai J. (2019). "AI blockchain platform for trusting news", inProc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul., pp. 1610-1619.

III. PROPOSED METHODOLOGY

The proposed system is designed to provide secure online transactions using cloud technology, OTP verification, and encryption techniques. Initially, users register and log in to the system using their credentials.

When a user initiates a transaction, the system generates an OTP and sends it to the registered email or mobile number. Along with the OTP, detailed transaction information such as product details and payment amount is sent to the user.

If the transaction is legitimate, the user enters the OTP to complete the process. If the transaction is unauthorized, the user can avoid sharing the OTP and use the provided security link to report the fraud to cybercrime authorities.

All user data and transaction details are encrypted and stored securely in the cloud database. This ensures data confidentiality and prevents unauthorized access. The system combines authentication, encryption, and real-time alerts to provide a robust security framework.

IV.SYSTEM DESIGN AND IMPLEMENTATION DETAILS

IV.1 User Module

This module allows users to register, log in, and perform online purchases. Users can browse products, add them to the cart, and proceed with payment using secure methods.

IV.2 OTP Authentication Module

During transactions, an OTP is generated and sent to the user. The transaction is completed only after successful OTP verification, ensuring secure authentication.

IV.3 Mail Confirmation Module

The system sends transaction details such as product name and amount to the user's email. This helps users verify whether the transaction is genuine**.**

IV.4 Security Link Module

If a fraudulent transaction is detected, the user can click the security link provided in the email to report the issue to cybercrime authorities immediately.

IV.5 Encryption and Cloud Storage Module

All sensitive data is encrypted before storing in the cloud database. Cloud storage ensures scalability, data backup, and secure access.

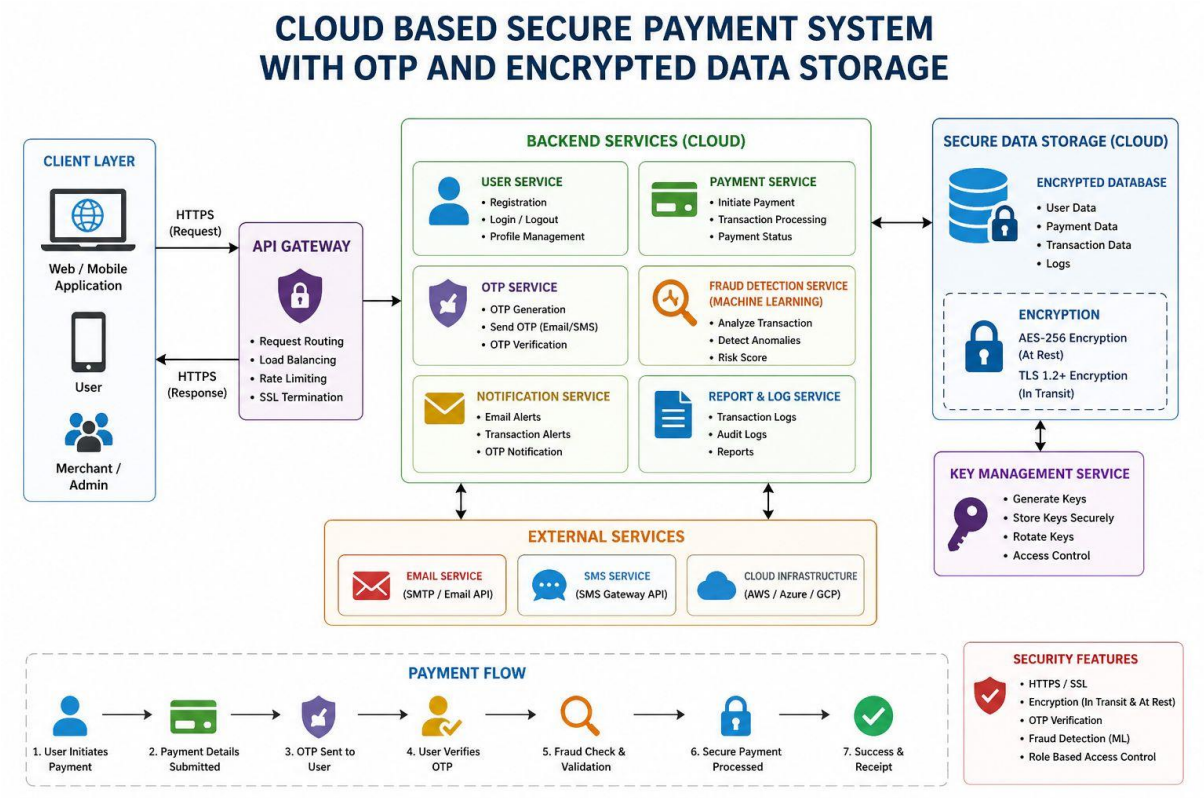
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15654

IV.6 System Architecture



The Cloud Based Secure Payment System is designed using a multi-layer architecture to ensure security and smooth transaction processing. The system starts with the user interface, where users access the application through web or mobile. The request is sent to the backend server using secure HTTPS protocol.The backend (application server) handles important functions like user authentication, payment processing, OTP generation, and fraud detection. When a user makes a payment, an OTP is generated and sent through email or SMS for verification. Only after entering the correct OTP, the transaction will be completed.

V.RESULT AND DISCUSSION

The proposed system effectively reduces the risk of OTP fraud and unauthorized transactions. The integration of email alerts and security links provides users with better awareness and control over their transactions.

Encryption techniques ensure that sensitive data remains secure, while cloud-based implementation provides high availability and scalability. Compared to existing systems, the proposed model offers improved security, faster response to fraud, and enhanced user trust.

VI.CONCLUSION

The cloud-based secure payment system with OTP and encrypted data storage provides an efficient solution to address security challenges in online transactions. By combining OTP authentication, email verification, encryption, and fraud reporting mechanisms, the system ensures secure and reliable payment processing.

The proposed system minimizes cyber threats, protects user data, and enhances trust in digital payment platforms. It can be widely implemented in e-commerce and banking systems to improve overall security.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15654

Future Directions

The Future improvements may include biometric authentication, AI-based fraud detection, and blockchain integration for enhanced transparency and security in financial transactions.

REFERENCES

[1]. de Oliveira N. R., Pisa P. S., Lopez M. A., de Medeiros D. S. V., and Mattos D. M. F., (2021).”Identifying fake news on social networks based on natural language processing: Trends and challenges",Information, vol. 12, no. 1, pp. 38.

[2]. Vijay J. A., Basha H. A. and Nehru J. A. (2021). “A dynamic approach for detecting the fake news using random forest classifier and NLP”, in Computational Methods and Data Engineering. Springer, pp. 331-341.

[3]. Nikiforos M. N., Vergis S., A. Stylidou A., Augoustis A., Kermanidis, K. L and Maragoudakis, M. (2020). “Fake news detection regarding the Hong Kong events from tweets", in Proc. Int. Conf. Artif. Intell. Appl. Innov. Greece: Springer, pp. 177-186.

[4]. Kumar S., Asthana, R. Upadhyay S., Upreti, N. and Akbar M., “Fake news detection using deep learning models: A novel approach", (2020). Trans. Emerg. Telecommun. Technol., vol. 31, no. 2, p. e3767.

[5]. Sansonetti G., Gasparetti F., D'Aniello G., and Micarelli A. (2020. “Unreliable users detectionn in social media: Deep learning techniques for automatic detection", IEEE Access, vol. 8, pp. 213154-213167.

[6]. Ochoa I. S., Mello G. D.,Silva L. A, Gomes A. J., Fernandes A. M. R., and Leithardt, ``FakeChain V. R. Q. (2019). “A blockchain architecture to ensure trustin social media networks” in Proc. Int. Conf. Qual. Inf. Commun. Technol.Algarve, Portugal: Springer, pp. 105-118.

[7]. Shae Z. and Tsai J. (2019). “AI blockchain platform for trusting news”, inProc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jul., pp. 1610-1619.

[8]. Paul S., Joy J. I., Sarker S., Shakib H., Ahmed S., and Das A. K.(2019). ”Fakenews detection in social media using blockchain" in Proc. 7th Int. Conf.Smart Comput. Commun. (ICSCC), pp. 1-5.

[9]. Qayyum A., Qadir J., Janjua M. U., and Sher F. (2019). “Using blockchain to reinin the new post-truth world and check the spread of fake news", IT Prof., vol. 21, no. 4, pp. 16-24.

[10]. Golbeck J., Auxier B., and Kori V. (2018). “Fake news vs satire: A dataset andanalysis", in Proc. 10th ACM Conf. Web Sci., pp. 17-21.