International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Encrypted Life Insurance Verification Portal with Public Access and Audit Trails

Gone Ishwarya, Ankam Hindu*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Ankam Hindu

ABSTRACT

The rapid growth of digital insurance services has increased the need for secure information management, controlled user access, and protected communication among administrators, agents, and clients. Insurance platforms manage highly sensitive data, including customer details, policy information, financial transactions, and confidential documents, making strong security and efficient system management essential. However, many existing insurance management systems rely on conventional web applications with limited security features, manual processing, and inadequate monitoring. These limitations often result in unauthorised access, poor workflow management, insecure document handling, and reduced operational transparency. Furthermore, the lack of encrypted communication, structured audit mechanisms, and role-based authorisation increases security risks and affects overall system reliability. To overcome these challenges, this work presents a secure web-based insurance management system developed using the Flask framework for application development and request handling. Tiny Database (TinyDB) is used to maintain customer information, policy records, encrypted documents, payment details, notifications, communication logs, and audit records. The system implements Role-Based Access Control (RBAC) to provide separate privileges for administrators, insurance agents, and clients**.** ElGamal encryption is employed to secure file storage and message exchange, while password hashing protects user authentication credentials. Additional features include automated premium calculation, policy comparison, secure file upload and download, notification management, and activity logging. Experimental implementation demonstrates that the proposed framework enhances data confidentiality, operational efficiency, transparency, and secure workflow management, providing a reliable and scalable solution for modern digital insurance platforms.

Keywords: Digital Insurance System, Role-Based Access Control (RBAC), ElGamal Encryption, Flask Framework, Secure Data Management.

1.INTRODUCTION

In recent years, health insurance coverage has increased significantly across the world as governments and private organisations continue to promote affordable healthcare services. In developed countries such as the United States, a large majority of the population is covered by health insurance, enabling better access to medical treatment and contributing to improved health outcomes, lower mortality rates, and enhanced quality of life [1]. Individuals without adequate insurance coverage often face financial burdens and limited access to healthcare, which may negatively affect their physical, mental, and economic well-being. Therefore, comprehensive health insurance plays a vital role in ensuring a healthier and more secure lifestyle [2]. Health insurance is provided through both public and private organizations, where an agreement is established between the insurance provider and the policyholder. Under this agreement, the insurer covers eligible medical expenses, including hospitalization, accidental injuries, disabilities, and other healthcare costs, while the policyholder pays regular premium amounts to maintain coverage. A high percentage of uninsured individuals places additional pressure on

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

healthcare systems because many postpone essential medical treatment and rely on emergency services, resulting in increased healthcare costs and inefficient resource utilization.Traditionally, the health insurance claim process was only partially automated and involved extensive paperwork, repeated visits to insurance offices, and lengthy claim verification procedures. These manual operations consumed considerable time and resources while increasing the likelihood of human errors during claim auditing and document management [3]. In addition, paper-based claim records were more susceptible to unauthorized modifications, creating opportunities for fraud and reducing transparency among insurance providers, healthcare service providers, and policyholders. With the advancement of digital technologies, health insurance claim processing has become increasingly electronic, improving the efficiency and reliability of insurance services. Digital insurance platforms simplify communication between policyholders and insurers, accelerate claim verification, support automated auditing, minimise fraudulent activities, reduce operational costs, and eliminate the need for frequent physical visits [4,5].

2. LITERATURE SURVEY

Rangel, et al. [6] presented for the first time the implementation of an asymmetric encryption algorithm called ElGamal based on spiking neural P systems and their cutting-edge variants. The proposed design involves the encryption and decryption processes. Specifically, they proposed the design of a neural network to efficiently perform the Extended Euclidean Algorithm used in the decryption task. Annamalai, et al. [7] studied and designed a Slime Mold Optimization with ElGamal Encryption with a Hybrid Deep-Learning-Based Classification (SMOEGE-HDL) model in an IoT environment. The proposed SMOEGE-HDL model mainly encompasses two major processes, namely data encryption and data classification. At the initial stage, the SMOE technique is applied to encrypt the data in an IoT environment. For optimal key generation in the EGE technique, the SMO algorithm has been utilized. Al-Zubaidie, et al. [8] devised a protocol that combines the Fernet (FER) algorithm with the ElGamal (ELG) algorithm. Additionally, they integrated Data Leakage Detection (DLD) technology to verify the integrity of keys, encryptions, and decryptions. The integration of these algorithms ensures that electronic-commerce transactions are both highly secure and efficiently processed. Their analysis indicated that the protocol outperforms the algorithms used in previous studies, providing superior levels of security and performance. Alotaibi, et al. [9] anticipated that this method will speed up computation time and simplify the encryption process per character without compromising security. The overall findings demonstrate that this method dramatically cuts down computation time and ciphertext enlargement while supporting the development of more flexible and effective cryptographic algorithms.

Adeniyi, et al. [10] employed RSA and ElGamal cryptographic algorithms with the application of SHA-256 for digital signature formulation to enhance security and validate the sharing of sensitive information. The goal of the study was to authenticate shared data using the SHA-256 hash function with RSA and ElGamal cryptographic algorithms. The methodology involved the implementation of these algorithms using the C# programming language. Amirkhanova, et al. [11] explored the security challenges posed by quantum attacks and proposed a novel quantum-resistant public-key encryption scheme based on ElGamal and the Short Integer Solution (SIS) problem. The proposed scheme provides security against both quantum and classical threats in modern cryptographic environments. Raghav, et al. [12]

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

proposed PB-TPRE, a threshold proxy re-encryption scheme with proactive properties. The shares of re-encryption keys are distributed to all proxies using Shamir Secret Sharing, and the proactive property enables renewal of the shares without changing the original secret, thereby providing resistance against collusion among proxies, users, and the cloud. Velmurugan, et al. [13] proposed a Cloud-based Decentralized Trust Management System (DTMS)-connected Efficient, Provably Secure Data Selection Sharing Scheme (EPSDSS). The EPSDSS approach employs Attribute-Based Encryption (ABE) and Proxy Re-Encryption (PRE) to provide fine-grained access control over shared data while improving participant accountability through decentralized trust management.

Wan, et al. [14] designed an improved ElGamal cryptosystem based on chaos synchronization. In the proposed system, the public key does not have to appear in the public communication channel, making the cryptosystem function like a symmetric encryption algorithm. A discrete sliding mode controller is used to synchronize the master and slave chaotic systems before applying the improved ElGamal cryptosystem, thereby reducing opportunities for attacks associated with static public keys. Wu, et al. [15] proposed an asymmetric scanning holography cryptosystem based on the ElGamal algorithm. The method encodes images using sine and cosine holograms, divides each hologram into a signed bit matrix and an unsigned hologram matrix, and encrypts both matrices using the sender's private key and the receiver's public key. The ciphertext matrices are then transmitted to the receiver, who decrypts them using the receiver's private key and the sender's public key.

3. PROPOSED SYSTEM

The proposed methodology as shown in Fig. 1 follows a structured and secure approach for developing a role-based digital insurance management framework that emphasizes data confidentiality, transparency, and operational reliability. The study integrates secure authentication, encrypted communication, controlled data access, and transaction monitoring into a unified workflow. A modular pipeline governs user interaction, data storage, cryptographic processing, and auditing, ensuring that sensitive insurance information is protected throughout its lifecycle. Lightweight storage mechanisms and server-side control logic support efficient data handling, while continuous logging and notification processes enable real-time monitoring and accountability. This methodology ensures that insurance operations remain secure, traceable, and scalable in real-world digital environments.

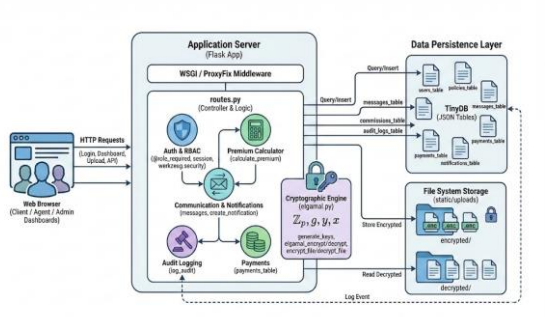

Fig.1: System architecture for life insurance verification portal.

Flask Web Server (app.py, routes.py)

- The Flask backend acts as the core control layer of the system.
- It handles authentication, session management, and role-based access validation.
- Requests related to policies, payments, encrypted messages, and files are routed to appropriate handlers.
- The server coordinates interactions between cryptographic modules, the database, and the user interface.
- Administrative actions such as audits, exports, and monitoring are also managed at this layer.

TinyDB Database (lic_database.json)

- TinyDB stores all persistent records required for system operation.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

- It maintains structured collections for users, policies, payments, commissions, messages, files, audit logs, and notifications.
- The database enables fast read/write access while maintaining a lightweight footprint.
- Its JSON-based storage format enhances portability and ease of deployment in small to medium-scale environments.

User and Policy Data Input

- User-generated data such as registration details, policy information, payment records, and messages form the primary input sources.
- Uploaded documents such as policy files and supporting records are treated as sensitive binary data.
- All inputs are validated at the server level before further processing.
- Sensitive inputs are routed through encryption pipelines prior to storage.

Cryptographic Processing Module (elgamal.py)

- The cryptographic layer manages secure key generation, encryption, and decryption.
- Public–private key pairs are generated for each user during registration.
- Messages and files are encrypted using the receiver's public key before storage.
- Decryption is performed only at the recipient side using the private key.
- Base64 encoding ensures safe handling of encrypted binary data.

Secure Messaging and File Handling

- Encrypted messages are stored in the database without exposing plaintext content.
- Uploaded files are encrypted before being written to disk storage.
- Access to encrypted files is strictly controlled through role and ownership checks.
- Decryption occurs dynamically during authorized download requests.

Audit Logging and Notification Engine

- Every critical system activity such as login attempts, policy creation, file access, and payment updates is logged.
- Audit records capture timestamps, user identity, actions performed, and IP address details.
- Notifications are generated for events like new messages, policy creation, and payment updates.
- Read/unread tracking ensures user awareness and interaction feedback.

Payment and Commission Management

- Payment records are created automatically during policy generation.
- Payment status transitions from pending to paid based on authorized actions.
- Agent commissions are calculated and stored upon policy issuance.
- Financial records are logged and linked with audit trails for traceability.

Secure Output and Data Retrieval

- Authorized users can retrieve policies, payments, messages, and files through controlled endpoints.
- Decrypted outputs are generated only for permitted users and sessions.
- Retrieved data is displayed through the interface and optionally exported in CSV format.
- All retrieval operations contribute to the audit and monitoring cycle.

3.1 ElGamal Encryption

ElGamal encryption is an asymmetric cryptographic technique that secures data using a public–private key pair derived from modular arithmetic. It relies on the computational difficulty of the discrete logarithm problem to ensure confidentiality. During encryption,

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

randomness is introduced for every message, making identical plaintexts produce different ciphertexts. This probabilistic behaviour strengthens resistance against pattern analysis attacks. ElGamal supports encryption of both textual and binary data by processing information in blocks. It is widely used in secure communication systems where key sharing must be avoided.

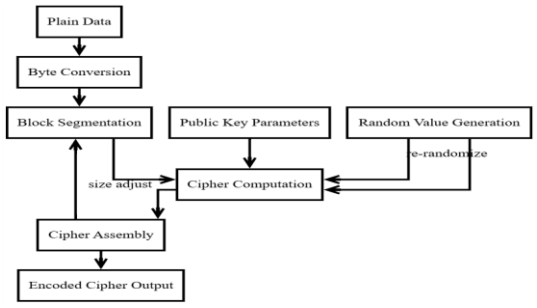

Fig. 2: Internal workflow of ElGamal encryption.

Message Preparation: The Fig. 2 workflow starts by taking plaintext as input and then converted into a byte sequence. Large messages are divided into manageable blocks suitable for modular arithmetic. This ensures compatibility with the mathematical constraints of the algorithm.

Public Key Parameter Extraction: The encryption process retrieves the public key components required for computation. These parameters define the cryptographic group used for encryption. Only public information is accessed at this stage.

Random Value Generation: A cryptographically secure random value is generated for each message block. This value introduces non-determinism into the encryption process. It ensures that ciphertexts differ even for repeated plaintexts.

Cipher Component Computation: Using modular exponentiation, two cipher components are computed for each block. One component represents the randomized key exchange element, while the other masks the plaintext. These values together form the encrypted output.

Block-wise Cipher Assembly: Encrypted components from all blocks are collected and structured. Metadata such as block length is attached to preserve reconstruction accuracy. This step ensures correct alignment during decryption.

Encoding for Storage or Transmission: The assembled ciphertext is encoded into a safe transport format. Encoding ensures compatibility with storage systems and communication channels. The final encoded output represents the encrypted message.

4. RESULTS AND DISCUSSION

The Encrypted Life Insurance Verification Portal is implemented as a web-based application using a structured backend architecture to manage users, policies, secure communication, and audit monitoring. The system follows a RBAC where administrators, agents, and clients access different functionalities through controlled authentication mechanisms. Flask is used to handle routing, request processing, and session management, while TinyDB serves as a lightweight database for storing system records such as users, policies, encrypted files, messages, and audit logs. Encryption technique ElGamal is integrated to protect sensitive communications and file transfers within the system. Secure file handling and encrypted messaging ensure confidentiality during data exchange. Audit logging tracks user activities to maintain transparency and accountability. Notification mechanisms support real-time updates for system events.

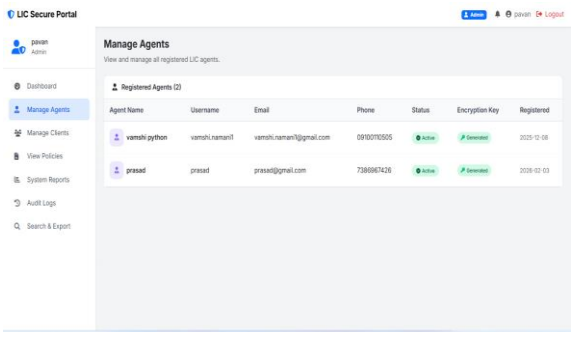

Fig. 3: Agent Management Interface of the Secure Insurance Portal.

Received: 30-05-2026 | Accepted: 01-07-2026 | Published: 08-07-2026

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Fig.3 depicts the agent management interface available to administrators within the secure insurance portal. The interface presents a structured overview of all registered agents, including their usernames, contact details, account status, encryption key availability, and registration information. It reflects the administrative capability to supervise agent accounts and verify readiness for secure operations. The interface also emphasizes controlled access and monitoring of agent participation within the system.

Fig. 4 depicts the policy creation interface that allows agents to generate new insurance policies for registered clients within the secure insurance portal. The interface represents the structured collection of policy information including client selection, policy type, coverage amount, premium value, policy duration, and beneficiary details. It reflects built-in validation rules such as minimum coverage requirements and automatic commission calculation. The view also indicates secure handling of policy-related data and automated client notification after policy creation.

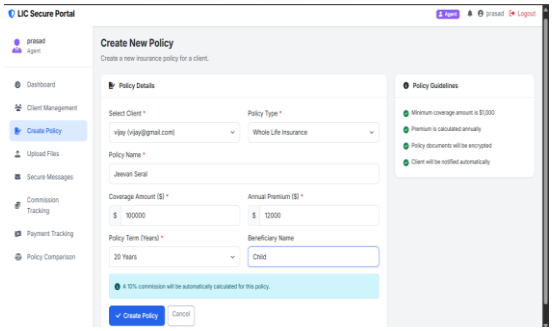

Fig. 4: Policy Creation Interface for Agents in the Secure Insurance Portal

Fig. 5 depicts the updated client management interface available to agents after successful policy creation within the secure insurance portal. The interface reflects real-time updates in client association status, indicating assigned clients and corresponding policy counts. It presents essential client details along with actionable options for creating additional policies and uploading encrypted files. The displayed confirmation message highlights successful workflow execution and system feedback.

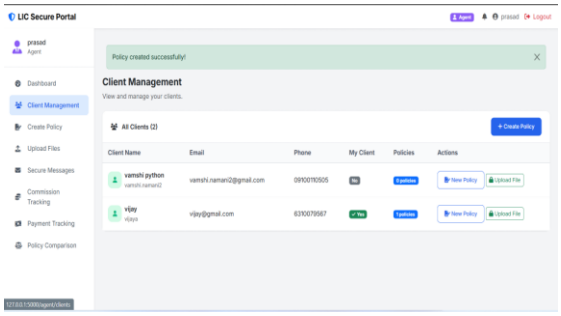

Fig. 5: Updated Client Management Interface Showing Policy Assignment Status

Fig. 6 depicts the secure communication interface that enables clients to exchange encrypted messages with agents and administrators within the insurance portal. The interface represents message composition, recipient selection, and encrypted message transmission using ElGamal cryptography. It also displays received messages with clear indication of encryption and successful decryption status at the client side. The view reflects controlled access to confidential communication and ensures that only authorized recipients can read message content.

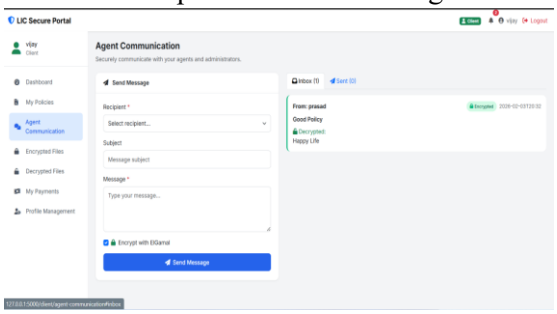

Fig. 6: Client–Agent Secure Communication Interface

Fig. 7 depicts the payment tracking interface that allows clients to monitor premium payment details within the secure insurance portal. The interface presents a summary of pending and paid amounts along with a detailed payment history linked to specific policies. It reflects the client's ability to track payment status, due dates, and premium types in a transparent manner. The structured presentation supports

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

timely payment awareness and financial accountability.

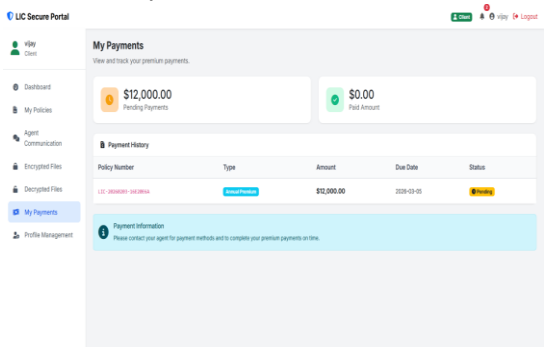

Fig. 7: Client Payment Tracking Interface

Fig. 8 depicts the profile management interface that enables clients to update and manage their personal and beneficiary information within the secure insurance portal. The interface presents editable personal details along with beneficiary information required for policy association. It also reflects the status of cryptographic keys, indicating active public keys and secured private keys for encrypted operations. The view highlights account status and membership information to provide transparency to the client.

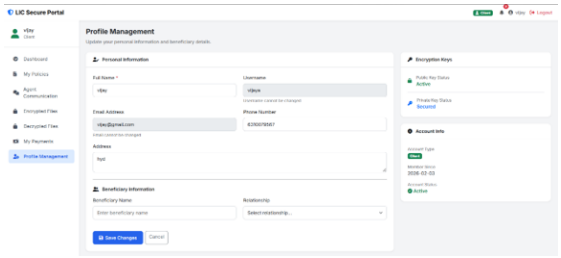

Fig. 8: Client Profile Management Interface

Fig. 9 depicts the payment tracking interface available to agents for monitoring premium payments collected from clients within the secure insurance portal. The interface presents a summarized view of pending payments, collected payments, and total invoices generated. It reflects detailed payment records linked to specific policies and clients, including payment amount, due date, and payment status. The confirmation message indicates successful recording of payment transactions and real-time system feedback.

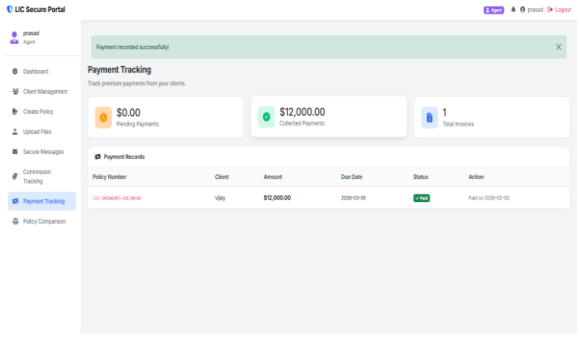

Fig. 9: Agent Payment Tracking Interface

Fig. 10 depicts the policy comparison and recommendation interface that assists agents in evaluating multiple insurance policy options for clients within the secure insurance portal. The interface presents side-by-side comparisons of policy types along with key attributes such as coverage characteristics, benefits, and base premium rates. It reflects decision-support functionality that enables agents to recommend suitable policies based on client needs. The structured comparison view supports informed policy selection and efficient advisory services.

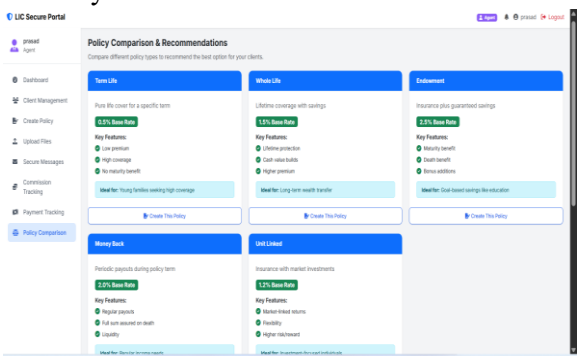

Fig.10: Policy Comparison and Recommendation Interface for Agents

Fig.11 depicts the audit log interface that enables administrators to monitor and review all system activities and user actions within the secure insurance portal. The interface presents a chronological record of events including user logins, payment updates, encrypted file downloads, and decryption activities along with corresponding timestamps and IP addresses. It reflects comprehensive tracking of critical operations to ensure accountability and traceability. The availability of export

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

functionality supports offline analysis and compliance reporting.

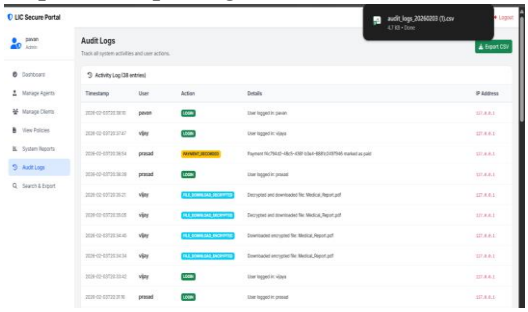

Fig. 11: Audit Log Monitoring and Export Interface or Administrators

5. CONCLUSION

This research successfully implements a secure, web-based insurance management framework that integrates role-based access control, encrypted communication, and lightweight data persistence into a unified system. By leveraging Flask for backend control, ElGamal encryption for protecting messages and documents, and TinyDB for efficient storage, the system ensures confidentiality, integrity, and traceability of sensitive insurance data. Performance improvements are achieved through modular architecture, lightweight database operations, and selective encryption applied only to critical data, reducing unnecessary computational overhead. Optimized request handling and session management enable faster response times during authentication, policy access, and data retrieval. The use of asymmetric encryption strengthens security while maintaining acceptable performance for real-time user interactions. Audit logging and notification mechanisms further enhance operational reliability and transparency. The system demonstrates improved efficiency compared to manual or unsecured digital approaches by minimising data leakage risks and streamlining insurance workflows.

REFERENCES

[1] Rajawat, A.S.; Bedi, P.; Goyal, S.B.; Shaw, R.N.; Ghosh, A.; Aggarwal, S. Ai and blockchain for healthcare data security in smart cities. In AI and IoT for Smart City Applications; Springer: Singapore, 2022; pp. 185–198.

[2] Li, J.; Lan, Q.; Zhu, E.; Xu, Y.; Zhu, D. A Study of Health Insurance Fraud in China and Recommendations for Fraud Detection and Prevention. J. Organ. End User Comput. 2022, 34, 1–19.

[3] Lavanya, S.; Kumar, S.M.; Kumar, P.M. Machine Learning Based Approaches for Healthcare Fraud Detection: A Comparative Analysis. Ann. Rom. Soc. Cell Biol. 2021, 25, 8644–8654.

[4] Huang, X.; Wu, B. Impact of urban-rural health insurance integration on health care: Evidence from rural China. China Econ. Rev. 2020, 64, 101543.

[5] Saldamli, G.; Reddy, V.; Bojja, K.S.; Gururaja, M.K.; Doddaveerappa, Y.; Tawalbeh, L. Health care insurance fraud detection using blockchain. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 145–152.

[6] Rangel, I.; Vázquez, D.-E.; Vázquez, E.; Duchen, G.; Avalos, J.-G.; Sanchez, G. First ElGamal Encryption/Decryption Scheme Based on Spiking Neural P Systems with Communication on Request, Weights on Synapses, and Delays in Rules. Mathematics 2025, 13, 1366. https://doi.org/10.3390/math13091366

[7] Annamalai, C.; Vijayakumaran, C.; Ponnusamy, V.; Kim, H. Optimal ElGamal Encryption with Hybrid

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Deep-Learning-Based Classification on Secure Internet of Things Environment. Sensors 2023, 23, 5596. https://doi.org/10.3390/s23125596

[8] Al-Zubaidie, M.; Shyaa, G.S. Applying Detection Leakage on Hybrid Cryptography to Secure Transaction Information in E-Commerce Apps. Future Internet 2023, 15, 262. https://doi.org/10.3390/fi15080262

[9] S. Alotaibi, K. Alharbi, B. Abaalkhail, and D. M. Ibrahim, "Sensitive Data Exposure: Data Forwarding and Storage on Cloud Environment," Int. J. online Biomed. Eng., vol. 17, no. 14, pp. 4– 18, 2021, doi: https://doi.org/10.3991/IJOE.V17I14.27365

[10] Adeniyi, E.A.; Falola, P.B.; Maashi, M.S.; Aljebreen, M.; Bharany, S. Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions. Information 2022,13, 442. https://doi.org/10.3390/info13100442

[11] Amirkhanova, D.S.; Iavich, M.; Mamyrbayev, O. Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles. Cryptography 2024, 8, 31. https://doi.org/10.3390/cryptography8030031

[12] Raghav, Andola, N., Verma, K. et al. Proactive threshold-proxy re-encryption scheme for secure data sharing on cloud. J Supercomput 79, 14117–14145 (2023). https://doi.org/10.1007/s11227-023-05221-3

[13] Velmurugan, S., Prakash, M., Neelakandan, S. et al. Provably secure data selective sharing scheme with cloud-based decentralized trust management systems. J Cloud Comp 13, 86 (2024). https://doi.org/10.1186/s13677-024-00634-8

[14] Wan, P.-Y.; Liao, T.-L.; Yan, J.-J.; Tsai, H.-H. Discrete Sliding Mode Control for Chaos Synchronization and Its Application to an Improved El-Gamal Cryptosystem. Symmetry 2019, 11, 843. https://doi.org/10.3390/sym11070843

[15] Wu, C.; Ding, Y.; Yan, A.; Poon, T.-C.; Tsang, P.W.M. Asymmetric Optical Scanning Holography Encryption with Elgamal Algorithm. Photonics 2024, 11, 878. https://doi.org/10.3390/photonics11090878

[16] Kumar, Anuj. "Optimization of Process Parameters in Metal Additive Manufacturing for Defect Reduction Using Machine Learning." International Journal of Engineering Research and Science & Technology, Vol. 14, No. 1, 2018, pp. 41-60