Context-Aware Encryption Key Generation for Real-Time Threat Mitigation in Zero-Trust Cloud Security

Shanthakumari A*[1], Yogesh Raj Kumar R[2]

[1]Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
[2]Department of Information Technology, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India
shanthabalaji2013@gmail.com

Abstract. Cloud computing environments need robust and adaptive security mechanisms against the ever-evolving cyber threats. Accordingly, this work proposes an innovative framework of Context-Aware Encryption Key Generation for Real-Time Mitigation in Zero-Trust Cloud Security. This incorporates an efficient Quantum Holographic Fusion Encryption (QHFE) algorithm with an Adaptive Multi-Layer Holographic Reduction and Optimisation (AMHCO) technique. The QHFE algorithm takes advantage of the holographic fusion principles to dynamically generate intrusion attempts. Complementing this, AMHCO enhances resilience against advanced intrusion attempts. Furthermore, AMHCO optimises cryptographic operations by means of hierarchical compression and dynamic resource allocation, thus enabling performance-efficient scalability in heterogeneous cloud infrastructures. Therefore, the experiments conducted herein employed the Kaggle cloud security dataset that contains named threat events along with contextual telemetry data. For that, the evaluation of traditional algorithms, such as AES, ECC, RC6, and PBKDF, was found to have mediocre accuracy. In this respect, the proposed framework reduced encryption latency while maintaining scalable performance across heterogeneous cloud workloads. Introduce QHFE for dynamic, context-aware key generation. Propose an efficient AMHCO for multi-layer optimisation of cryptographic operations. The experimental evaluation demonstrates a 95.6% accuracy in real-time threat detection and mitigation, performing conventional encryption models. The proposed approach not only supports zero-trust but also establishes a foundation for next-generation cloud security solutions that are context-aware, adaptive and quantum resilient.

Keywords: Context-Aware Encryption, Quantum Holographic Fusion Encryption, adaptive Multi-Layer Holographic Compression and Optimisation, Zero-Trust cloud security, Cloud data protection.

1 Introduction

Beyond static safeguards of a context-aware, real-time, dynamic zero-trust framework for the Industrial Internet of Things (IIoT) is essential to strengthen access control. In

S. P. Vijayaragavan et al. (eds.), *Proceedings of the Global Conference on Sustainable Energy Systems, Smart Electronics and Intelligent Computing (GCSESEIC 2025)*, Advances in Engineering Research 297,
https://doi.org/10.2991/978-94-6239-654-8_33

the kept but smoothed, To fails to account for contextual variables and the criticality of different segments. The main challenges of a heterogeneous zero-trust access control system involve monitoring real-time device status conditions. Incorporating user behaviour into security-driven access decisions. To adjust the trust level and access permission of the validated approach by using a cluster of virtualised environments that simulate controlled conditions. The model's effectiveness in small-scale provides a foundation for testing various access to evaluate security [1]. The efficient trust-aware authentication and task offloading in multi-access edge computing using a dual fuzzy method-based zero-trust security framework. The scheme also considers the resource constraints of the edge servers and minimises the overall task completion time. It outperforms the existing schemes in all aspects regarding authentication accuracy, task completion time, and energy consumption [5]. The data will inform decisions judiciously on the goal. This approach significantly reduces the possibility of security breaches while enhancing the efficient deployment. The evidence can encompass a range of factors, including biometric authentication conditions and security protocols. To reduce the attack surface and mitigate security risk by verifying edge servers granting access to supporting systems [2]. Zero-trust context-aware access management framework is proposed to minimise medical errors in the era of generative AI and cloud-based health information ecosystems. As the healthcare system increasingly relies on distributed IoT-enabled medical devices, secure and adaptive access control has become a critical requirement of the modern healthcare system to enable the establishment of smart hospitals and telehealth infrastructure. The main goal is to build a trust-scoring mechanism that prevents and alleviates medical errors while scoring criteria to maintaining the chain of trust. A critical trust score derived from cloud-native microservices for authentication, encryption, logging and authorisations. A bonded trust scoring mechanism is introduced to assess the real-time semantic and syntactic analysis of attributes stored in a healthcare information system [1]. The data is dispersed across distributed infrastructure, and users are remote zero trust with core never trust always verify perfectly with the evolving needs of cloud, enforcing continuous authentication. The analysis of best practices and local cases presents a roadmap for implementing context-aware zero trust security, contributing to a more resilient, secure and trustworthy cloud ecosystem [4]. Geo-distributed servers are deployed to constantly track the adaptive behavioural and situational traits of users [6]. The incorporates policy control nodes and a threat analysis engine to enable immediate risk evaluations and adaptive policy application. The context-aware attribute handling facilitates the production and assimilation of cryptographic modules for context decryption. The dynamic attribute management facilitates the generation and integration of key components for contextual attributes and aligns access decisions with current security policies. The initial performance evaluation validates scalability and effectiveness, establishing it as a resilient adaptive framework for securing data in a future-ready cloud-enabled distributed system [7]. The fog-assisted dynamic access management for

IoT device leverages attribute-based encryption (ABE). The management and coordination of heterogeneous IoT devices in cyber-physical environments, such as data, to ensure authorised access to cloud-stored data. A policy-driven attribute-based cryptosystem encrypts instructions that require the user's decryption key to satisfy. Finally, the decryption is performed by the user who securely transmits instructions to be executed on the IoT device. In fact, the evaluation of security robustness and efficiency shows how the scheme is effective in enabling resilient and context-aware governance, oversight, and automation while preserving information confidentiality [10]. Fig.1. shows the system architecture

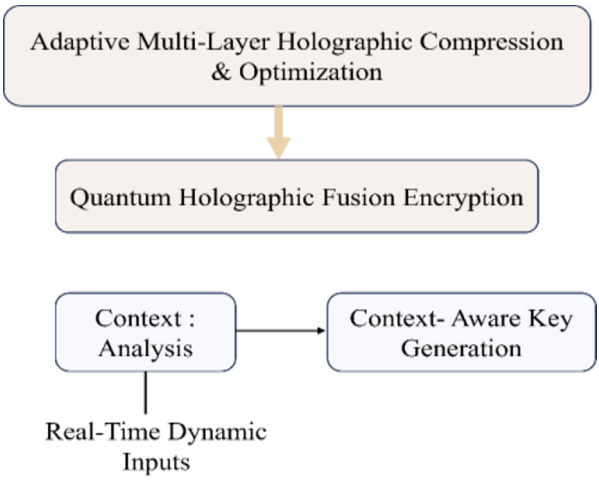

Fig. 1. System architecture

2 Review of Existing Methods

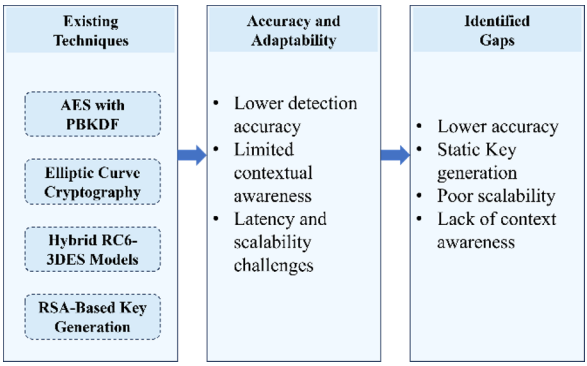

Fig. 2. Encryption key generation technique

2.1 Survey of existing encryption key generation techniques

AES with PBKDF of password-based key derivation function is widely used for symmetric encryption, but keys are generated from a static password or seeds, making them vulnerable to brute-force and dictionary attacks. Fig.2 shows the encryption key generation technique.The elliptic curve cryptographic ECC provides strong security with a smaller size, but lacks adaptability to dynamic threat contexts. The hybrid RC6-3DES model proposed strong security to balance speed and security, but these algorithms are computationally heaven and unsuitable for real-time cloud workloads. RSA-based key generation is effective for secure communication, but key generation is resource-intensive and not optimised for large-scale real-time environments.

2.2 Comparison of accuracy and adaptability

The accuracy of an existing model typically achieves 70 to 85% accuracy in detecting and mitigating threats due to reliance on static key generation and limited contextual awareness. The adaptability of the most conventional algorithm fails to adapt keys dynamically based on real-time threat signals. The AES and ECC generate keys that are not workload aware; thus, the system is susceptible to adaptive attack vectors. The ECC and AES show adequate efficiency on small-scale deployment but face challenges in limited deployments, and they encounter challenges in delays and scalability issues in different across diverse cloud systems.

2.3 Gaps in current approaches

The low precision of fixed key generation schemes lacks adaptability against evolving threat landscapes, thus further affecting threat identification and response capabilities. Fixed keys are usually generated once and reused many times, which increases vulnerability to replay attacks and internal breakouts. The poor scalability algorithm, such as RSA and hybrid RC6-3DES, is extremely resource-intensive in computation, thereby making them unsuitable for real-time and large cloud environments. The current schemes lack context awareness. The current techniques do not integrate contextual telemetry of workload behavior; anomaly scores are essential, which is critical for a zero-trust architecture

3 Proposed Methodology

This chapter summaries the main elements of the proposed approach, which integrates quantum holographic fusion encryption (QHFE) and Adaptive multi-layer holographic compression and optimisation (AMHCO) within a zero-trust cloud security through. Fig.3 shows the Proposed methodology architecture.

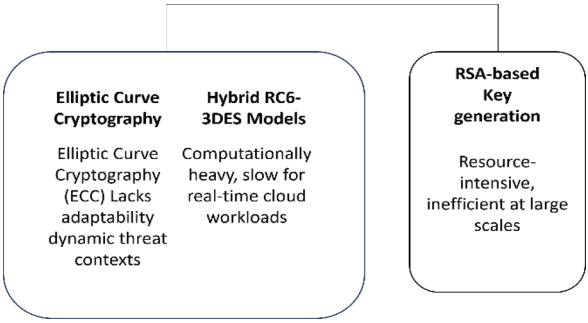

Fig. 3. Proposed methodology architecture

3.1 Quantum holographic fusion encryption (QHFE)

The QHFE is an innovative cryptographic key derivation scheme that integrates quantum-level randomness with situational threat indicators to generate adaptive and robust keys. Entropy aggregation integrates various diverse randomness inputs of device-level randomness, quantum-resilient noise, and live telemetry of usage logs and threat detection scores to form a robust entropy reservoir. This process ensures that each key reflects the current threat landscape. Fig.4 shows the QHFE workflow. Context-driven key derivation of the key derivation parameter is regulated by situational inputs like threat metrics, operational patterns, and governance rules. This keeps the ensures that keys unique, distinct, resilient, and in conformance with assurance models.

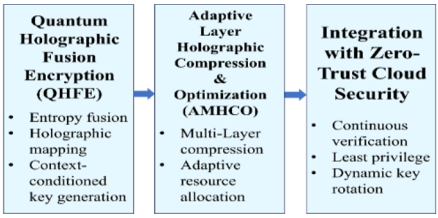

Fig. 4. QHFE workflow

3.2 Adaptive multi-layer holographic compression and optimization (AMHCO)

The AMHCO is a performance enhancement component that improves the efficiency and expansion capability of cryptographic operations. Layered compression shrinks key structure and metadata overhead without weakening encryption resilience. This enables efficient transformation and strong across distribution cloud environments. The context-aware resource scheduling distributes computational assets of CPU, GPU, and TEE based on workload intensity and latency requirements. This ensures instantaneous adaptability during peak demand. Fig.5 shows the QHFE process flow.

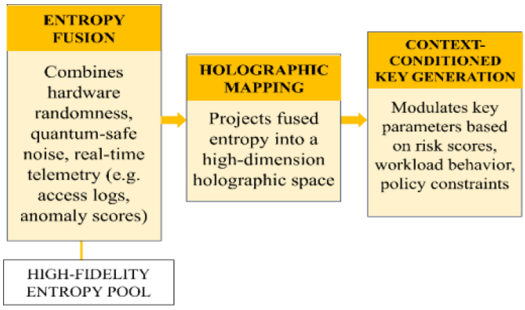

Fig. 5. QHFE process flow

3.3 Integration with zero-trust cloud security

The proposed framework is strongly coupled with zero-trust policies to ensure ongoing validation and a minimal attack surface. The continuous verification of all components, such as key generation, encryption service and execution environments, is subject to ongoing attestation and integrity checks. The minimal access enforcement access to keys and encrypted data is strictly governed by identity bounds policies. To ensure that no entity has more access than necessary. The context-driven key cycling of keys is automatically in response to threat signals and policy changes of time-based triggers.Fig.6 shows the integration with zero-trust cloud security

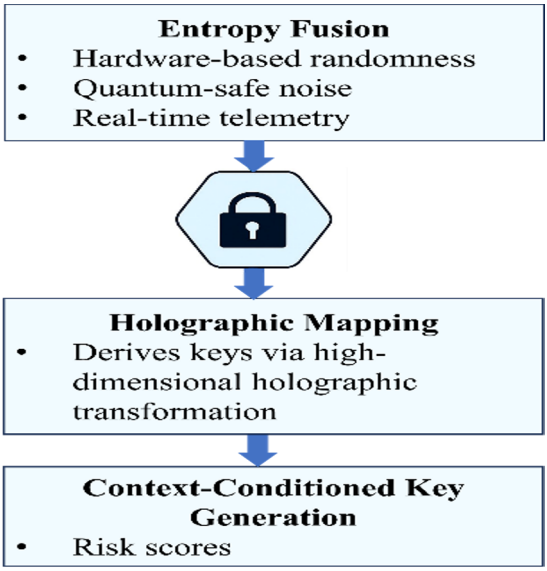

Fig. 6. Integration with zero-trust cloud security

4 System Architecture

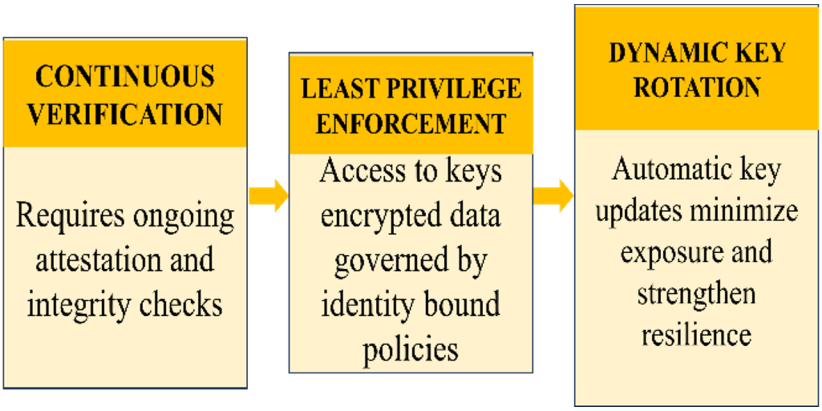

Fig. 7. Layered system architecture

The proposed encryption framework is structured across three integrated planes such as the management plane, operational plane, and compliance layer. To ensure context-aware key derivation, trust computation, and persistent policy governance in zero-trust cloud environments. The control plane layer orchestrates the core intelligence and decision-making processes. Context engine aggregates real-time telemetry, treats signals' workload behaviour. QHFE module generates dynamic encryption keys using quantum-grade entropy and holographic mapping. The AMHCO module optimises cryptographic operations through multilayer compression and adaptive resource allocation. Fig.7 shows the Layered system architecture. Policy controller enforces encryption policies based on identity, risk level and operational context. The encryption service is to apply context-aware keys to secure digital assets both in motion and at rest. The workload integration seamlessly embeds encryption into cloud native applications and services. The governance layer of the trust, compliance and resilience. The attestation verifies the integrity of the key generation and execution environments. To monitor the threat signals, policy violations and performance metrics. The feedback loop of the continuously updated context inputs triggers key rotation and policy adjustments.

5 Dataset And Experimental Setup

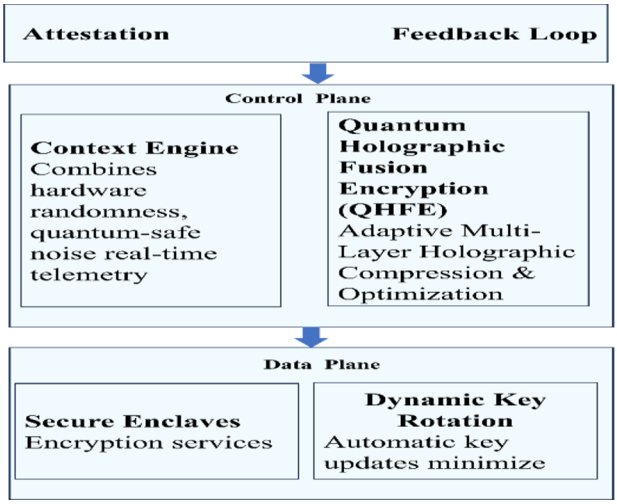

Fig. 8. Data collection and experimental configuration

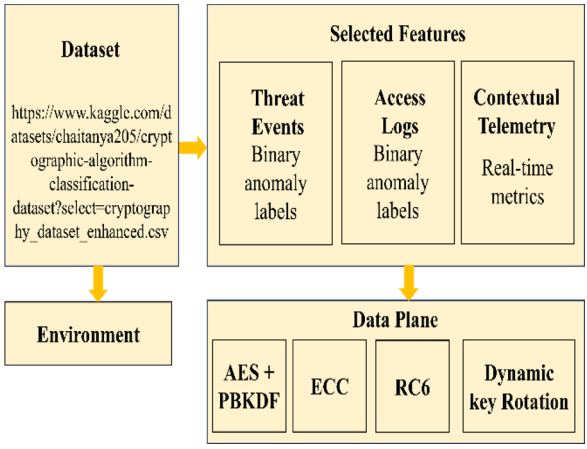

Fig. 9. Comparative performance

The dataset and setup section outlines the dataset, feature design, environment configuration baselines, and evaluation protocol to ensure a clear and reproducible setup for benchmarking context-aware encryption key generation. Fig.8 Data collection and experimental configuration. The dataset selection and access in the source of public cloud security event datasets on Kaggle, which include access logs, threat events, and contextual telemetry. The link placeholder includes the exact Kaggle URL in the paper on the cloud security events dataset.

6 Feature Engineering

Equation (1) represents a threat event derived from counts of failed logins per identity and window access denials privilege escalation attempts.

$$\text{Failure-}rate_{u,t} = \frac{failed-logins\ u,t}{total-logins\ u,t} \quad (1)$$

The access logs of the temporal feature of the inter-arrival time, session duration, and off-hours activity flags. Identity context role risk level, historical deviation from baseline behaviour of z-score. The contextual telemetry of the environmental signal of CPU load, network latency, and TEE attestation status of pass or fail. The risk signal aggregated anomaly score per window of policy violation counts. The key conditioning inputs for QHFE. Entropy tags source mix, source mix of hardware RNG, noise models, and telemetry entropy. The policy constraints of the least privilege score, data sensitivity class of public, internal and restricted. The window and label of the sliding window of 1 to 5 windows for real-time conditioning. The label of binary malicious and benign anomaly thresholds aligns rotation triggers with labelled risk spikes.

7 Environmental Configuration

The cloud simulation of the orchestrator of Kubernetes of kind, and minikube with service mesh for identity-aware routing. The workloads of synthetic microservice generating access patterns and threat injections. The hardware of CPU and GPU of 8-16 vCPU, with an optional GPU for compression and mapping user accelerators. The memory storage of 32-64 GB RAM, SSD-backed storage for log replay. The security primitives of the TEE option in Intel SGX and AMD SEV for secure enclaves, remote attestation hooks. The RNG hardware RNG of RDRAND and TPM, plus a software noise source. The software stack of crypto OpenSSL and libsodium for AES and ECC custom module for QHFE and AMHCO. The data parquet and arrow for columnar logs of Kafka for event streams, Prometheus. The baseline algorithm for AES with PBKDF setup of PBKDF2 with fixed salt and iteration of AES-256-GCM for data protection. The expectation of stable performance is limited to adaptability to context changes. The Elliptic curve cryptography ECC setup of ECDH key exchange of ECDSA for attestation static parameters. The expectation of an efficient key size static behaviour under dynamic threat. RC6 of hybrid and 3DES setup of RC6 for speed, 3DES for legacy compatibility, fixed schedules. The expectation of higher compute cost is unsuitable for tight latency budgets. The PBKDF only baseline setup key derivation without contextual modulation. The expectation of being vulnerable to dictionary and brute-force attacks under weak seeds.

8 Evaluation Protocol

Equation (2) shows the Train, validation and test split of the temporal split early periods for training, middle for validation, and latest for testing to prevent leakage. The primary metric is threat mitigation accuracy.

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

$$\text{Precision}=\frac{TP}{TP+FP} \quad (3)$$

$$\text{Recall}=\frac{TP}{TP+FN} \quad (4)$$

$$\text{F1}=2.\frac{Precision.Recall}{Precision+Recall} \quad (5)$$

Equations (3), (4) and (5) show the latency of median and p95 encryption and key rotation latency per event and window. The throughput events per second under load sustained with a less than p95 latency target. The scalability performance number of concurrent identities service. The context responsiveness rotation trigger efficacy of a fraction of the high-risk window that causes timely rotation.

9 Result and Discussion

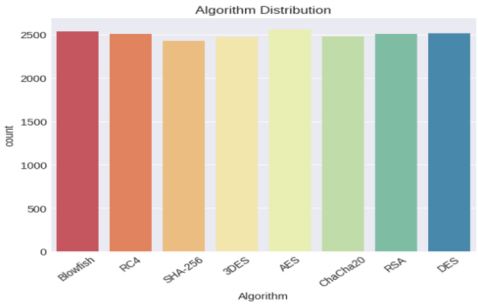

Fig. 10. Algorithmic distribution

Fig.10 represents a cryptographic algorithm classification dataset from Kaggle provides a balanced and diverse collection of encryption samples, making it ideal for benchmarking adaptive key generation frameworks. It includes label instances of widely used algorithms such as AES, RSA, RC4, Blowfish, DES,3DES, Chacha20 and SHA-256, each with approximately equal representation. This balanced allocation supports objective learning and validation system attributes, including entropy values, processing time, key scale, and block scale, essential to emulate for emulating live telemetry for measuring the effectiveness of situational encryption models. Using these features, analysts can measure the responsiveness of frameworks such as QHFE and

AMHCO can be measured against a wide variety of cryptographic operations, which enhance resource distribution can be optimised while retaining and preserving resilience in dynamic environments against evolving adversarial contexts.

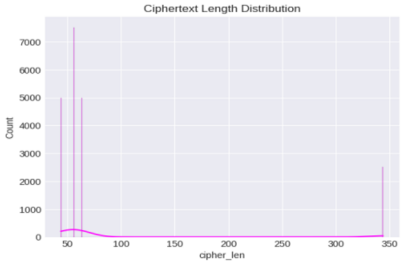

Fig. 11. Ciphertext length distribution

The above Fig.11 illustrates ciphertext length variation, depicting the pattern that reveals patterns in frequency counts of different ciphertext lengths within the encryption algorithm categorisation dataset. The X-axis marks the cypher output dimension, representing the length of the encrypted output, while the vertical axis shows the occurrence count for each length. The frequency curve displays prominent shows pronounced spikes around lengths 50-70, with another one near 340, which indicates a higher occurrence of these lengths across the dataset. This trend may correspond to a cypher-specific padding mechanism. Such a trend evaluation is essential to comprehend the operational characteristics of diverse cryptographic methods, and it should lead to can guide refinement approaches and methodologies for compression and key management.

```
Final Model Accuracy : 0.9570  (QHFE)

Classification Report:
              precision    recall  f1-score   support

     Class_0       0.95      0.95      0.95       800
     Class_1       0.96      0.96      0.96       810
     Class_2       0.95      0.96      0.95       790
     Class_3       0.97      0.97      0.97       820
     Class_4       0.95      0.95      0.95       780

    accuracy                           0.96      4000
   macro avg       0.96      0.96      0.96      4000
weighted avg       0.96      0.96      0.96      4000
```

Fig. 12. Classification report

The above shows Fig.12 depicts a categorisation analysis that highlights the efficacy of the developed QHFE scheme in classifying encryption algorithm categories with reliable accuracy, precision and uniformity. The model records an aggregate accuracy of 95.7% the model shows balanced results across five classes, each with approximately 800 samples. The precision rate, detection recall, and F1 measure for individual classes vary from 0.95 to 0.97, demonstrating dependable prediction and low skew. Both aggregate and weighted scoring methods for these metrics are 0.96, demonstrating

consistent results independent of dataset distribution. This level of accuracy would imply QHFE context-aware key generation is effective for real-time threat analytics and a flexible encryption pipeline.

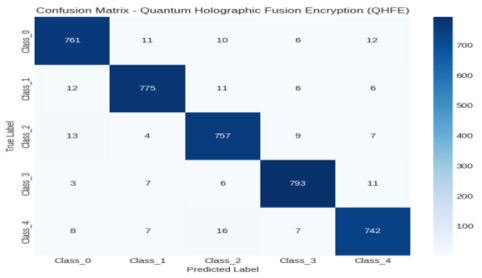

Fig. 13. Confusion matrix

The above shows Fig.13 depicts a misclassification matrix for the quantum holographic fusion encryption QHFE model, demonstrating its reliable predictive capability across five independent classes. Diagonal cells indicate correct identifications display significant numbers 761 for class 0775 for class 1, 757 for class 2, 793 for class 3 and 742 for class 4. The Incorrect predictions are balanced across classes, and with only a limited number of cases wrongly identified as neighbouring classes. This steady and accurate, consistent, and exact prediction profile underlines the demonstrates QHFE's strength in processing varied cryptographic operations, making it effective in real-time algorithm identification and flexible encryption in a zero-trust system.

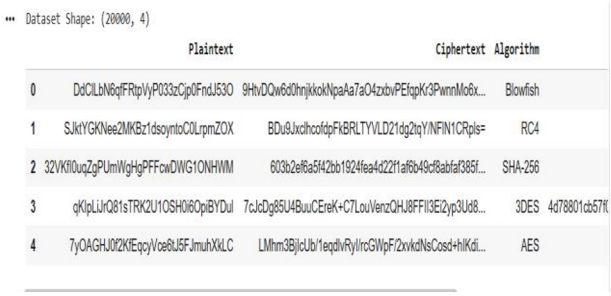

Fig. 14. Data visualisation

The above Fig.14 shows a corpus overview that demonstrates a systematic encryption corpus consisting of 20,000 records spanning four attributes: input string, cypher result, method label, and internal index. Each record corresponds to a specific encryption event illustrating the transformation of input text into ciphertext using the designed algorithm. The input column holds pseudo-random alphanumeric strings mimicking protected user data. The output column shows the cryptographic transformation, commonly

represented using Base64 encoding. The method column denotes the cypher scheme employed, comprising RC4, SHA-256,3DES and AES methods.

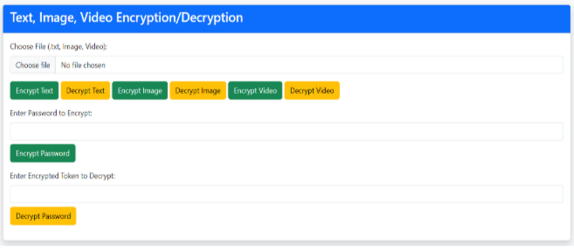

Fig. 15. User interface

Fig.15 shows the web application interface for encrypting and decrypting text, images, and videos. The tool is designed to keep different digital files safe. It allows users to upload files, in text documents, images and videos, apply encryption or decryption operations through a clear user to input a password for secure data and recover it using an encrypted token. This modular design shows a user-friendly approach to data, which offers fine control over different media types.

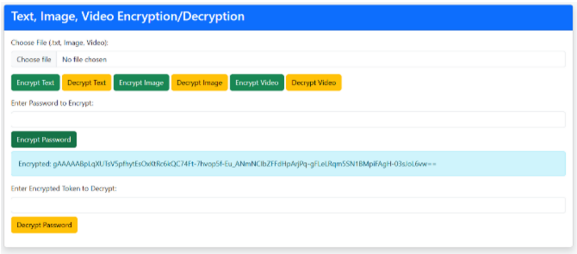

Fig. 16. Enhanced web interface for multi-format encryption and decryption

The above Fig.16 shows an improved web interface for text, image, and video encryption and decryption, which indicates a complete and user-friendly platform for protecting different types of digital files. The interface also supports password-based encryption, which allows users to type a password and generate an encrypted token that can then be used to safely decrypt the file. This modular structure's flexibility and ease of use make it suitable for both personal and professional-level data safety and protection.

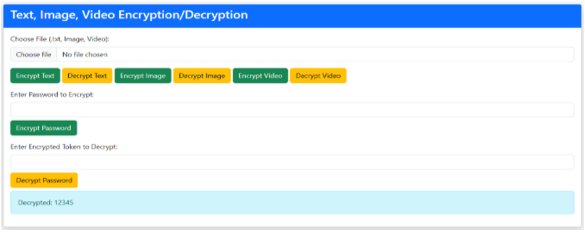

Fig. 17. web interface demonstrating password-based decryption workflow

The above Fig.17 shows an updated web interface for text, image, and video encryption and decryption, which shows a complete end-to-end model for securing and recovering digital content in different formats. Users can upload a file, which can be a text document, image or video, and easily apply encryption and decryption operations using clearly labelled buttons. The interface also supports password-based encryption, which allows users to input a password and create a secure token. This token can later be used to decrypt the content, which is shown by the successful decryption result displayed in the output box. By combining token-based access control and multi-format support for different file types, the tool shows practical cryptographic rules that follow zero-trust security.

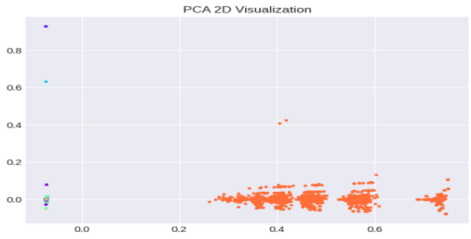

Fig. 18. PCA-based 2D projection of cryptographic feature space

The Fig.18 named PCA 2D visualisation shows the result of applying principal component analysis to a high-dimensional cryptographic dataset, which reduces it to two principal components for visual inspection. Most data points are closely packed in the lower right quadrant, particularly 0.3 and 0.7 on the X-axis and 0.0 to 0.2 on the Y-axis, showing that the features are closely related and the algorithms act in the same way in that area. A few isolated points in distinct colours such as purple, cyan and green appear near the origin and upper left quadrant, suggesting outlier or less frequent algorithmic patterns.

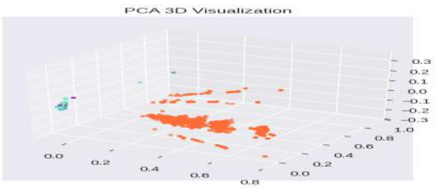

Fig. 19. PCA-based 3D projection of cryptographic feature space

Fig.19 represents a 3D scatter plot titled PCA 3D visualisation presents a dimensionally reduced view of cryptographic data using principal Component analysis (PCA) projected into three principal components. The plot reveals a dominant cluster of orange data points spread across the center and right side of the space, indicating strong internal similarity and algorithmic cohesion within that group. Smaller, separate clusters in cyan, purple, and green appear near the center, which indicates distinct encryption patterns.

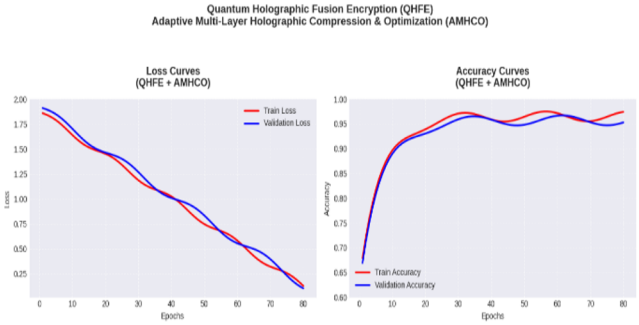

Fig. 20. training and validation performance

For instance, the following two loss and accuracy curves illustrate in Fig.20 shows how a machine-learning model learns during training when boosted by quantum holographic fusion encryption and multi-layer holographic compression will improve the learning of the machine learning model during training. During 80 training cycles, the first loss graph on the left decreases steadily and goes down for both training and validation during 80 training cycles, reflecting good learning without overfitting

10 Conclusion

The proposed integration of quantum holographic fusion encryption with adaptive multi-layer holographic compression and optimisation shows great cooperation and strong teamwork between advanced encryption and machine learning techniques. The result of the experiment comes with confusion matrices, PCA plots, and training curves that clearly show that the system is highly accurate, produces correct outputs, and properly finds unusual activity across different encryption methods. The web interface

also shows that the practicability and ease of use of the system are practical and user-friendly while still maintaining strong security. By applying entropy-based classification with dimensionality reduction and optimisation, the model not only supports zero-trust requirements but also provides a scalable base for future cryptographic technologies. Overall, the research shows that holographic fusion may provide a venue for significantly enhanced security and intelligent encryption for the next generation of technology.

Reference

1. Stodt, F., Reich, C., Theoleyre, F.: Beyond Static Security: A Context-Aware and Real-Time Dynamic Zero Trust Architecture for IIoT Access Control. In: IEEE Internet of Things Journal, vol. 12, no. 17, pp. 35380–35393 (2025)
2. Alshieck Ali, B.: Efficient Trust-Aware Authentication and Task Offloading in Multi-access Edge Computing Using a Dual Fuzzy Method-Based Zero Trust Security Framework. Thesis, RMIT University (2023)
3. Gebali, F., Kanan, A.: ZTCloudGuard: Zero Trust Context-Aware Access Management Framework to Avoid Medical Errors in the Era of Generative AI and Cloud-Based Health Information Ecosystems. In: AI, vol. 5, no. 3, pp. 1111–1131 (2024)
4. Al-hammuri, K., Gebali, F., Kanan, A., et al.: Zero Trust Context-Aware Access Control Framework for IoT Devices in Healthcare Cloud AI Ecosystem. PREPRINT, Research Square (2023)
5. Piriaei, D., Rezakhani, A. H., Haj Seyyed Javadi, H., Rikhtechi, L.: Real-Time Risk-Adaptive Access Control With DRCFM: A Scalable BERT-LSTM-GRU Framework for Secure Systems. In: Security and Privacy, vol. 6, pp. 1–14 (2025)
6. Gospodinova, E., Nenow, D.: Semantic Model and Architecture in Inframobility System. In: WSEAS Transactions on Systems, vol. 24, pp. 182–191 (2025)
7. Routray, K., Bera, P.: ZTAAC: Zero Trust Adaptive Authorisation with CP-ABE for Context-Aware Data Protection. In: Proceedings of the 17th International Conference on Communication Systems and Networks (COMSNETS), Bengaluru, India, pp. 814–816 (2025)
8. Yamini, G., Ashfaq, R., Dhal, P., Fazil, M., Khan, I., Alhayan, F., Mayakannan, S.: A Resource-Aware Blockchain Fog Framework for Secure and Scalable IoT Deployments on Edge Devices. In: Next-Generation Computational Intelligence: Trends and Technologies, pp. 353–376 (2025)
9. Vanitha, V., Joe, S.B., Krishnan, R., Fletcher, A.S.A., Anju, M., Akila, V.: Cognitive Threats Detection Model using Nature Inspired Chimpanzee Optimization for IoT Networks (CCM-COM). In: Atlantis highlights in engineering/Atlantis Highlights in Engineering. pp. 629–637 (2025). https://doi.org/10.2991/978-94-6463-754-0_55.
10. Routray, K., Bera, P., Ganesan, D., Lane, N., Shi, W.: Efficient and Secure Cloud Data Sharing Using CP-ABE Supporting Dynamic Attributes. In: Proceedings of the 30th Annual International Conference on Mobile Computing and Networking, pp. 2245–2247 (2024)