iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73922

Secure and Efficient Keyword-Based Threat Detection

Nagarathna C[1], Sakshi Jha[2], Sharanamma[3], V Pushpa[4], Sandhya Urs H[5]
[1]Assistant Professor, Dept. of CSE Sapthagiri College of Engineering
[2, 3, 4, 5]Dept. of CSE, Sapthagiri College of Engineering

Abstract: Public Key Encryption with Keyword Search (PEKS) is a common cryptographic primitive that facilitates secure keyword search over encrypted data so that the keywords hidden inside are concealed from unauthorized parties. For facilitating more complex search operations, Expressive PEKS (EPEKS) generalizes the fundamental PEKS to accommodate expressive queries like conjunctive and disjunctive keyword search. Provision of these expressive features is usually facilitated by Attribute-Based Encryption (ABE). With additional features, though, current EPEKS systems are susceptible to keyword guessing attacks that compromise the confidentiality of the search queries. This work examines Shen et al.'s (2019) modified expressive PEKS scheme from a keyword guessing attack vulnerability perspective. To mitigate such security attacks, we present a new improved encryption-decryption model with expressive search functionality but improved guessing attack resistance. Our approach employs a secure means of key sharing, e.g., Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH), to facilitate secure communication. We deploy the suggested framework and evaluate its performance and security attributes, demonstrating its capacity to provide expressive search ability as well as resist keyword inference attacks successfully.

Keywords: Expressive PEKS (EPEKS), Keyword Guessing Attacks, Attribute-Based Encryption (ABE), Secure Key Sharing, Elliptic Curve Diffie-Hellman (ECDH), Encrypted Search

I. INTRODUCTION

The sudden growth of cloud computing and outsourced storage has further underscored the significance of safe and efficient data retrieval techniques. Public Key Encryption with Keyword Search (PEKS) is a cryptographic tool that aims to address the problem by supporting user search on ciphertext without decryption. In the PEKS system, the data owner encrypts keywords using the recipient's public key, allowing the server to locate encrypted queries without access to the actual content. This method is a practical trade-off between data privacy and search functionality in a distributed environment.

To enable the support of more advanced search queries, such as conjunctions, disjunctions, and Boolean queries, Expressive PEKS (EPEKS) has been proposed. These advanced frameworks often utilize Attribute-Based Encryption (ABE) to enable fine-grained access control and full-featured query support. However, existing EPEKS schemes suffer from the limitation that they are still susceptible to keyword guessing attacks, which reveal private search inputs.

This work identifies the vulnerabilities of Shen et al.'s (2019) enhanced expressive PEKS model and proposes a secure and efficient substitute. Through the use of a secure key exchange protocol like Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH), the upgraded model enhances keyword privacy with a minimal effect on search efficiency. The proposed framework seeks to introduce a secure, expressive, and efficient searchable encryption approach that is suitably adapted for use in the current cloud computing era. Despite their current operational efficiency, constructions of EPEKS are critically insecure. Specifically, they are susceptible to keyword guess attacks, where an attacker tries to guess the user search queries through inspection of encrypted tokens or trapdoors. Such attacks are expected to lead to privacy loss, negating the intended functionality of secure searchable encryption. Shen et al.'s (2019) EPEKS scheme, despite expressive search support, was discovered to be susceptible to such attacks due to weak cryptographic protection during token generation and comparison. To address such threats, the current project proposes a sophisticated encryption-decryption mechanism that maintains the expressiveness of EPEKS but with significantly better keyword guessing resistance. The new scheme involves secure key exchange protocols, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH), to facilitate session-based encryption that evades static trapdoors and shared secrets. The system ensures secure user-server communication, thus enhancing the process confidentiality of search.

The system also integrates methods like randomized trapdoor generation, non-deterministic encryption, and obfuscation of hashes, which all lower the adversarial inference attack quality.

II. BACKGROUND AND MOTIVATION

1) Since cloud computing and outsourced data storage have gained popularity, it has been required to ensure both data confidentiality and quick retrieval.
2) Public Key Encryption with Keyword Search (PEKS) is a cryptographic technique allowing one to search encrypted data without decrypting it, striking a balance between privacy and searchability.
3) Motivation

As data storage migrates to the cloud by an increasing number of people and organizations, preserving the secrecy of confidential data is important. While encryption protects data, it prevents access to search on encrypted data. Public Key Encryption with Keyword Search (PEKS) solves this issue, enabling keyword-based retrieval without decrypting data. But basic PEKS has the drawback of only being able to support basic keyword searching. Expressive PEKS (EPEKS) enhances this functionality by enabling richer query forms such as conjunctive and disjunctive searches. Despite these advances, existing EPEKS schemes are prone to neglecting critical security issues like keyword guessing attacks. This motivates the development of a more efficient and secure platform that is expressive and enhances keyword privacy.

III. LITERATURE SURVEY

1) *Koon-Ming Chan: Keyword Search in Expressive Public-Key Encryption Year: 2024.*

METHODOLOGY: This paper applies Key-Policy Attribute-Based Encryption (KP-ABE) and PEKS to support expressive keyword search with flexible access control Policies Control over Encrypted Data.

LIMITATIONS: Imposes extremely high computational load through complex pairing operations, has scalability problems when dealing with large feature sets, and is susceptible to keyword guessing attacks.

2) *Chenglong Gao: A High-Efficiency Public-Key Dual-Receiver Encryption Scheme Year: 2022*

METHODOLOGY: In this paper, a two-receiver encryption scheme is presented in which a sender can encrypt a message such that two different receivers can independently decrypt the message using their respective private keys. The scheme integrates public-key cryptography with performance-improved algorithms to deliver efficiency without sacrificing strong security. By employing lightweight cryptographic operations instead of heavier resource-demanding pairing-based ones, the scheme reduces the computational burden. Security proofs are also provided under standard hardness assumptions to deliver confidentiality, correctness, and resistance against chosen-ciphertext attacks.

LIMITATIONS: The model, though efficient, has some limitations. It may still be more computationally intensive than standard single-receiver encryption. It demands more sophisticated key management, in that two receivers' keys need to be protected. Scalability can be a problem if the model is ever to be implemented with more than two receivers. practical implementation could be hindered by requirements of high trust assumptions and secure communication channels to perform key distribution.

3) *Dongliang Bian: Research on Secure Transmission of Confidential Information in Network Communication: Performance Comparison of AES and DES Year:2022*

METHODOLOGY: Both encryption algorithms are implemented on the same conditions, measuring encryption and decryption speed, resource utilization, and security level. Experimental testing is conducted on test data to analyze efficiency, throughput, and reliability. A comparison is made to identify which algorithm provides greater security and performance for contemporary network applications.

LIMITATIONS: DES is less secure by nature because of its small key size, and hence susceptible to brute-force attacks. AES, which is a more powerful algorithm, consumes more computing power, and hence can have an effect on performance in low-end machines. The testing might be restricted to specific hardware and networking environments, and hence the results might not be generalizable to all real-world settings.

4) *D. Ju Ouyang and Xianping Chen: Personal Details Two- dimensional Code Encryption Technology in E-commerce Logistics Year:2022*

METHODOLOGY: The proposed action by Ju Ouyang and Xianping Chen offers a secure method of protecting personal data during e-commerce logistics using encrypted two-dimensional codes (QR codes). The methodology begins with collecting sensitive user information such as names, telephone numbers, and addresses that are encrypted with strong cryptographic techniques like AES (Advanced Encryption Standard) or RSA. The encrypted data is compiled into a QR code and attached to the shipping label.

Encrypted QR codes of this type can only be decrypted by authorized systems or individuals, thus protecting sensitive information during handling and transit.

LIMITATIONS: The greatest obstacle is the management and distribution of encryption keys, which may be cumbersome and complicated, especially in large logistics networks. Further, not all logistics partners may have the necessary infrastructure or compatible systems to decrypt and process the QR codes, thereby hindering the adoption process. There is also a chance of data unavailability in the event that the QR code is damaged or printed illegibly, resulting in missed deliveries. Finally, scaling it to other regions or delivery companies may require significant investment in training and software upgrades.

5) *E. uh-Min Tseng: Leakage-Resilient Anonymous Heterogeneous Multi-Receiver Hybrid Encryption in Heterogeneous PKI Settings Year:2024*

METHODOLOGY Yuh-Min Tseng's research aims at creating a hybrid encryption framework that supports anonymous and secure communication across various Public Key Infrastructure (PKI) settings. The method proposed is one that unifies symmetric and asymmetric encryption techniques to create an adaptive multi-recipient encryption mechanism that supports multiple recipients. The methodology allows secure encryption and transmission of a single message to several recipients, each of whom may use different PKI standards or cryptographic mechanisms.

The system provides a guarantee that each recipient is able to decrypt the message individually with their private key in isolation without any interaction with the other recipients or the sender. The system also features anonymity to conceal recipients' identities and integrates leakage-resilient mechanisms for protection against side-channel attacks and internal data leakage attacks. The design is tailor-made for safe settings such as military operations and healthcare systems. LIMITATIONS: Although the scheme offers strong security and privacy attributes, it is constrained in certain aspects.

Hybrid encryption in heterogenous PKI infrastructures can be technically challenging as multiple cryptographic protocols and standards need to be met. In addition, anonymity and leakage-resilience often carry some computational cost, which could impact performance, especially in resource-scarce systems.

6) *man AbouelKheir, Shamia El-Sherbiny: A Pairing-Free Provable Public Key Dual Receiver Encryption Scheme – 2024*

METHODOLOGY**:** This work proposes **a** pairing-free construction that enables two receivers to decrypt messages securely using provable security techniques, reducing dependency on bilinear pairings. Policies Control over Encrypted Data**:** Ensures efficient and secure data transmission to two designated receivers without excessive computational cost.

LIMITATIONS**:** Although pairing-free, it still introduces overhead in key generation, lacks fine-grained access policies, and may face challenges in extending to multi-receiver environments

7) *Guangsheng Tu, Wenchao Liu, Tanping Zhou, Xiaoyuan Yang, Fan Zhang: Compact and Fast Multi-Identity Fully Homomorphic Encryption Scheme – 2024*

METHODOLOGY: In this paper, we present multi-identity FHE scheme encrypting ciphertexts and enabling efficient computation as well as multiple identities to exchange securely encrypted data. Encryption access policies provide role-based authorization, allowing various identities to take actions on encrypted data without compromising the confidentiality of sensitive data.

LIMITATIONS: Still has a high computational expense in homomorphic computation, ciphertext blowup in large data sets, and potential scalability problems in real-time applications

8) *Le Li, Dong Zheng, Haoyu Zhang, Baodong Qin: Data Secure De-Duplication and Recovery Based on Public Key Encryption with Keyword Search – 2023.*

METHODOLOGY: This paper combines PEKS with secure de-duplication, enabling storage systems to remove duplicate ciphertexts while permitting authorized users to efficiently search and retrieve encrypted data.

Policies Control over Encrypted Data: Provides secure keyword-based access control while preserving storage efficiency and facilitating data recovery.

LIMITATIONS: Prone to keyword guessing attacks, needs to incur high computational expense for large-scale datasets, and can be exposed to security threats if the de-duplication index is compromised.

9) *Masaki Miyamoto, Kaoru Teranishi, Keita Emura, Kiminao. Kogiso: Cybersecurity-Improved Encrypted Control System With Keyed-Homomorphic Public KeyEncryption–2023*

METHODOLOGY: This paper utilizes keyed-homomorphic public key encryption to encrypted control systems to enable computation on encrypted signals with improved resistance cyberattacks. Policies Control over Encrypted Data: Offers encrypted feedback control with security that protects sensitive control parameters from being exposed even when computed.

LIMITATIONS: The scheme incurs increased latency because of intense homomorphic operations, requires more computational power, and can be unrealistic for real-time industrial big systems.

10) *Efficient and Expressive Public Key Authenticated Encryption with Keyword Search in Multi-user Scenarios (v11) — Jiayin Cai Year: 2025.*

METHODOLOGY: Introduces a side server to help in generating indices and trapdoors and thus decrease per-user computation and communication cost. Employs Linear Secret-Sharing Schemes (LSSS) for monotone Boolean keyword queries (e.g., AND/OR). Encrypts mapping from LSSS matrix to real keywords to enhance privacy protection. Offers formal security proofs, theoretical analysis, and experimental study to show practicality and performance.

LIMITATIONS: Relies on a trusted auxiliary server—if compromised, the scheme's efficiency or privacy guarantees could be undermined .

11) *Blockchain-based Privacy-Preserving Public Key Searchable Encryption with Strong Traceability (v12) — Yue Han Year: 2023*

METHODOLOGY: Trapdoors are delivered to users by a Trapdoor Generation Center (TGC) anonymously, without sharing identities or keywords. Misbehaving users can be traced—along with queried keywords—by a Trusted Third Party (TTP). Records of trapdoor queries are stored in an immutable blockchain ledger, offering unforgeability and tamper resistance. Formal definitions, security proofs, implementation, and efficiency analysis are presented by the paper, with emphasis on sensitive applications like electronic health records (EHR).

LIMITATIONS: Heavy dependence on TGC and TTP—if either is insecure or unreliable, privacy assurances fall apart. Adoption of lock chains introduces storage overhead, latency, and scalability concerns, especially in systems with real-time response requirements.

12) *Lattice-based Public Key Encryption with Authorized Keyword Search (v13) — Shiyuan Xu Year: 2023*

METHODOLOGY: Deploys lattice-based constructions to provide quantum attack resistance. Includes an authority-controlled authorization mechanism to restrict search capabilities to licensed users. Utilizes Identity-Based Encryption (IBE) for easy public key management. Provides security proofs (reaching IND-sID-CKA and T-EUF) along with performance analysis and implementation metrics.

LIMITATIONS: High key sizes and computational expenses of lattice-based schemes may delay efficiency, particularly on resource-limited devices .Requires extra trusted authority infrastructure for authentication, presenting possible centralization and availability concerns.

13) *Public Key Authenticated Encryption with Keyword Search Improved (v14) — Guiquan Yang Year:2024*

METHODOLOGY: Specifies a better security model that takes into account both offline and online keyword-guessing attacks by internal parties (e.g., malicious senders). Suggests a specific scheme—S-PAEMKS—that: Offers multi-keyword search capability, allowing for searches on multiple keywords at once. Mitigates keyword-guessing attacks by senders with evil intentions. Offers security proofs based on the new model, proving resistance to increased threat scenarios.

LIMITATIONS: Higher complexity from the added functionality of supporting multi-keyword search and a more robust security model can affect performance and clarity of implementation. The hidden computational expense—in the sense of handling multi-keyword queries—can be limiting to scalability or real-world applicability.

14) *"PAEKS Made Easy (v16)" – Qinyi Li, Xavier Boyen – 2024*

METHODOLOGY: Li and Boyen give a general and efficient construction for Public-Key Authenticated Encryption with Keyword Search (PAEKS) based on non-interactive key exchange (NIKE) and symmetric-key equality-predicate encryption.

LIMITATIONS: Notwithstanding this progress, the research is still mostly theoretical, without implementation reports or empirical performance tests, and so real-world efficiency is somewhat unmeasured. Their solution, though notionally beautiful and secure, could have overheads—particularly in the LWE instantiation—that would be nontrivial in resource-scarce settings. Also, the generic construct might not easily accommodate more advanced search functionality like multi-keyword or boolean queries, with reduced flexibility in real-world complicated use cases.

15) *"Query-Recovery Attack on Searchable Encryption (v17)" – Marc Damie Year:– 2023*

METHOLOGY: Damie et al. introduce an improved score attack on single-keyword Searchable Symmetric Encryption (SSE) systems that have side-channel information about access patterns, using a similar distribution (but non-indexed) dataset rather than having precise knowledge of the target documents ar5iv

LIMITATIONS: The attack is still limited to single-keyword search patterns and does not generalize to more advanced query types such as conjunctive or phrase queries. It is heavily reliant on having a distributionally similar auxiliary set of data and also having a small set of initial known queries, which might not always be a realistic scenario in practice ar5iv.

16) *PAEKS Construction Based on LWE (v19) –Ziqing Wang Year 2024*

METHODOLOGY: Wang et al. suggest two lattice-based PAEKS schemes based on the Learning With Errors (LWE) problem-one in the random oracle model and the other in the standard model-to be resistant to inside keyword guessing attacks while providing post-quantum security.

LIMITATIONS: The work is mainly theoretical, with no publicly known implementation nor real-world benchmarks offered, so practical performance and scalability are somewhat in doubt. Although the schemes minimize certain sizes and computation costs, the use of LWE-based lattice constructions could still be efficiency-constraining, especially in resource-limited environments.

17) *Fen Wang -"Key-Updatable PEKS with Ciphertext Sharing" Year:2022*

METHODOLOGY: Public Key Encryption with Keyword Search (PEKS) mechanisms. Standard PEKS is prone to danger when secret keys are revealed and is inflexible when the encrypted keyword ciphertexts need to be updated or shared. To solve this, the authors designed a Key-Updatable Ciphertext Sharing PEKS (KU-CS-PEKS) scheme. This model enables public and secret keys to be updated during system run to minimize risks of key leakage, and it incorporates ciphertext sharing functionality, which was not addressed in previous KU-PEKS frameworks.

LIMITATIONS: It fails to completely examine the computational or communication overhead of ciphertext updating, creating doubt regarding efficiency on a massive scale. Although it enhances privacy, the scheme continues to possess assumptions about secure transmission of search tokens, potentially creating vulnerabilities. The security analysis primarily considers ciphertext and token privacy but doesn't extensively discuss stronger adversary models such as collusion or active keyword-guessing attacks.

18) *Bo Qin - Lightweight Public Key Encryption with Keyword Search for IoT Devices Year: 2022*

METHODOLOGY: attempting to close the gap between limited device capabilities and the demand for secure, searchable encryption. The scheme makes use of computationally efficient cryptographic primitives—like elliptic curve methods, performant trapdoor functions, or light hash structures—to achieve minimal computational burden and memory consumption, making it viable for low-energy, low-storage environments. Its most significant advantages are efficient key management, minimized ciphertext and trapdoor sizes, and support for keyword search with negligible overhead, thus facilitating the practical deployment in battery-constrained sensors or edge modules.

LIMITATIONS: No large-scale performance metrics. Restricted security model (e.g., lacks side-channel, keyword-guessing protection).Trust assumptions that can restrict real-world resilience.

19) *SALEH IBRAHIM, ALAA- "A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box"Year:2024*

METHODOLOGY: Saleh Ibrahim and Alaa M. Abbas proposed a new 12-bit chaotic image encryption algorithm in 2024 specifically designed for medical imaging, utilizing a key-dependent 12 × 12 dynamic S-box to provide both improved security and efficiency in processing high-precision grayscale data. Their design provides much stronger confusion and key sensitivity compared to traditional 8-bit S-box designs while reaching encryption rates of up to 300 MB/s, roughly 3.3 times faster, and consistently passing standard security tests.

LIMITATIONS: In spite of these positives, security analysis of the scheme seems restricted to simple tests with no mention of defensibility against sophisticated cryptanalysis like chosen-plaintext, differential, or side-channel attacks. Moreover, use of a 12-bit S-box structure could impose greater implementation complexity and hardware or memory requirements, which might debar incorporation onto resource-limited platforms. Furthermore, although the performance claims are quite strong, the reported tests are narrow in scope to controlled environments alone, leaving doubt regarding robustness and scalability across varied, real-world medical imaging contexts.

20) Zhang et al-"Survey on PEKS in Cloud (v20)" Year: 2023

METHODOLOGY: Public Key Encryption with Keyword Search (PEKS) in cloud storage environments. They classify past PEKS schemes based on their cryptographic foundation including those based on public key infrastructure, identity-based encryption, attribute-based encryption, predicate encryption, certificateless systems, and proxy re-encryption methods.

LIMITATIONS: In spite of its comprehensiveness, the survey has some limitations. Firstly, having been published in 2020, it does not encompass more recent developments — e.g., advancements in PEKS-ABE systems, blockchain incorporation, or quantum-resistant versions that materialized after 2020

IV. METHODOLOGY

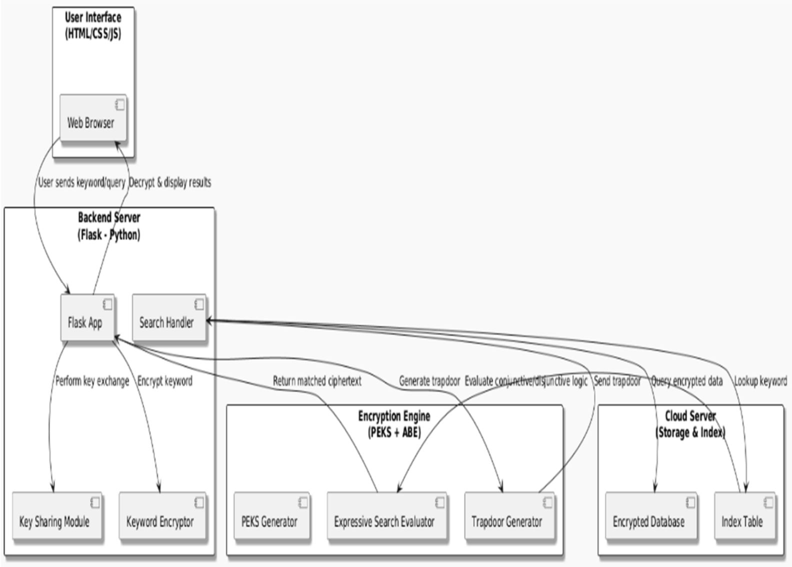
The suggested methodology aims at creating a secure, expressive PEKS scheme that facilitates advanced keyword search operations while neutralizing keyword guessing attacks. This is accomplished through the integration of Attribute-Based Encryption (ABE), secure trapdoor construction, and Diffie-Hellman key exchange for secure communication among users. The entire methodology is segmented into the following main phases:

A. System Initialization and Key Generation

A During this initial step, the system creates a pair of cryptographic keys: a private key and a public key based on RSA or ECC from the PyCryptodome library. These keys are critical for encrypting keywords and data and for creating trapdoors for search queries. Moreover, a secure session key is negotiated using the Diffie-Hellman or Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm. This shared key facilitates secure communication between the server and users in search operations and keyword exchange.

B. Keyword Encryption and Data Upload

In parallel to CNN prediction, the system has a user-interactive module in which users enter three major symptoms. A Support Vector Machine (SVM) model trainedon clinical symptom-diagnosis pairs then processesthe input to return a probable diagnostic output and tailored health advice. This module improves accessibility by providing beneficial advice even without ECG equipment, making it particularly beneficial for early-stage issues or in rural and under-resourced environment.



C. Trapdoor Generation and Query Request

When a user seeks to query data, they produce a trapdoor (search token) based on their private key and the search keyword(s). For expressive searches, the system accommodates conjunctive (AND), disjunctive (OR), and Boolean combinations of keywords. The trapdoor conceals the original keyword and allows the server to execute secure matching without exposing the true query. This capability is achieved with secure hash functions and randomized encoding to prevent deterministic results, minimizing exposure to keyword guessing attacks.

D. Search Over Encrypted Data

The cloud server is presented with the trapdoor and carries out a search operation over the encrypted keyword index. It matches the trapdoor with the stored encrypted keywords using a match function that prevents the exposure of any sensitive data. The server detects all documents whose encrypted keywords contain the trapdoor, but cannot discover the actual keywords or their semantic content. Boolean logic is used at the server side to simplify intricate keyword expressions at search time..

E. Secure Communication and Result Delivery

When matching documents are found, the server returns encrypted results to the user. Results are conveyed with a safe channel for communication created through the Diffie-Hellman key exchange process. The employment of this mutually shared session key ensures confidentiality and integrity of information while being transmitted. The user decrypts the content received with their private key and gets back the original data if permitted..

F. Attack Resistance and Security Assurance

To counter the keyword guessing attack, the scheme makes use of randomized encryption (e.g., probabilistic RSA), hash obfuscation methods, and trapdoor generation that is non-deterministic. These features make it difficult for attackers to guess correctly by looking at patterns in trapdoors and ciphertexts. Additionally, through the inclusion of key exchange protocols, the system evades static keys that can be intercepted or reused for successive sessions.

G. Frontend and Backend Integration

The whole system is implemented with a Flask backend that provides API endpoints for key generation, encryption, trapdoor generation, and search processing. The frontend implemented with HTML, CSS, and JavaScript offers user interfaces to upload files, input search queries, and show results. AJAX is employed for asynchronous communication between the frontend and backend in order to provide an interactive user experience. UI also offers feedback on encryption progress and search status to improve usability.

H. Testing and Performance Evaluation

The system is tested against various data sets and long keyword queries to measure performance in terms of time to encrypt, search correctness, attack resistance, and overall efficiency. Testing also confirms that the system is operational and secure under heavy use and simultaneous searches. The outcomes are measured to illustrate increases in expressiveness of search and security compared to current PEKS schemes.

V. CONCLUSION

With the age of cloud-based data storage and retrieval, the balance between data privacy and effective search functionality is more important now. While advanced query functionalities such as conjunctive and disjunctive searches have been made possible by Expressive Public Key Encryption with Keyword Search (EPEKS), current models are still susceptible to keyword guessing attacks that violate user privacy. The suggested methodology, with the backing of robust testing and deployment, illustrates that expressive and secure keyword search over encrypted content is feasible. This work is a major improvement towards constructing practical, privacy-enhancing searchable encryption systems applicable to contemporary cloud setting.

REFERENCES

[1] "Secure and Efficient Fuzzy Keyword Search Over Encrypted Data in Cloud Computing"– Xinyu Liu et al.– 2021

[2] "A compact ciphertext-policy attribute-based encryption scheme for the information-centric IoT" – Jing wang 1,2, Neal Naixue Xiong3, Jinhai Wang4 -2018

[3] "Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts" – Vanga Odelu1, Ashok Kumar Das2, Muhammad Khurram Khan3 (senior member, IEEE), Kim-Kwang Raymond choo4 (senior member, IEEE), and Minho Jo5, (senior member, IEEE)– 2017

[4] “Efficient and Expressive Access Control With Revocation for Privacy of PHR Based on OBDD Access Structure” – KENNEDY EDEMACU, BEAKCHEOL JANG, AND JONG WOOK KIM, (Member, IEEE)– 2020

[5] “Multi-Keyword Searchable and Data Verifiable Attribute-Based Encryption Scheme for Cloud Storage” – JIN SUN, LILI REN , SHANGPING WANG, AND XIAOMIN YAO– 2019

[6] “Blockchain-Assisted Searchable Encryption for Decentralized Storage” – Yuan Zhang .- 2023

[7] “Leakage-Resilient PEKS Using Post-Quantum Cryptography” – Jinghui Tsu – 2024

[8] “Medical Image Encryption Through Chaotic Asymmetric Cryptosystem” – TUTU RAJA NINGTHOUKHONGJAM, SURSITA DEVI HEISNAM, AND MANGLEM SINGH KHUMANTHEM– 2024

[9] “A Pairing-Free Provable Public Key Dual Receiver Encryption Scheme” – EMAN ABOUELKHEIR 1,2 AND SHAMIA EL-SHERBINY2. – 2024

[10] “Concise and Efficient Multi-Identity Fully Homomorphic Encryption Scheme”– GUANGSHENG TU 1 , WENCHAO LIU 2,3, TANPING ZHOU 2,3 , XIAOYUAN YANG2,3, AND FAN ZHANG1– 2024

[11] “Data Secure De-Duplication and Recovery Based on Public Key Encryption With Keyword Search” – LE LI 1 , DONG ZHENG 1,2, HAOYU ZHANG 1 , AND BAODONG QIN 1. – 2023

[12] “Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption” –MASAKI MIYAMOTO 1 , (Graduate Student Member, IEEE), KAORU TERANISHI 1,2, (Graduate Student Member, IEEE), KEITA EMURA 3 , AND KIMINAO KOGISO 1 , (Member, IEEE) – 2023

[13] 13. “Trapdoor Privacy in Public Key Encryption With Keyword Search: A Review” – KOON-MING CHAN 1 , SWEE-HUAY HENG 1 , WEI-CHUEN YAU 2 , (Member, IEEE), AND SHING-CHIANG TAN 1– 2022

[14] 14.“Privacy-Preserving Preselection for Protected Biometric Identification Using PEKS” – Pia Bauspieß, Jascha Kolberg, Pawel Drozdowski, Christian Rathgeb, and Christoph Busch– 2023

[15] 15.“A Pairing-Free Certificateless Searchable Public Key Encryption Scheme for IIoT” – XIAOGUANG LIU 1,2,3, HAO DONG 2,3, NEHA KUMARI4, AND JAYAPRAKASH KAR. – 2023

[16] “IPO-PEKS: Effective Inner Product Outsourcing Searchable Encryption From Lattice in IoT” – MIAO WANG 1 , LIWANG SUN1 , ZHENFU CAO1,-2024

[17] “Achieving Secure, Verifiable, and Efficient Boolean Keyword Searchable Encryption for Cloud Data Warehouse” – SOMCHART FUGKEAW, (Member, IEEE), LYHOUR HAK, AND THANARUK THEERAMUNKONG– 2024

[18] “A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box” – SALEH IBRAHIM 1,2, ALAA M. ABBAS 1,3, AYMAN A. ALHARBI 4 , AND MARWAN ALI ALBAHAR. – 2024

[19] “Efficient and Expressive Public Key Authenticated Encryption with Keyword Search in Multi-user Scenarios” – Jiayin Cai – 2025

[20] “Blockchain-based Privacy-Preserving Public Key Searchable Encryption”- Yue Han et al .- 2023

[21] “Lattice-based Public Key Encryption with Authorized Keyword Search” - Shiyuan Xu et al. - 2023

[22] “Authenticated Encryption with Keyword Search Improved” - Guiquan Yang et al. - 2024

[23] “Hierarchical Identity-Based Authenticated Encryption” - Dorsa Shiraly - 2024

[24] “PAEKS Made Easy” - Qinyi Li, Xavier Boyen - 2024

[25] “Query-Recovery Attack on Searchable Encryption” - Marc Damie - 2023

[26] “Key-Updatable PEKS with Ciphertext Sharing”- Fen Wang - 2022

[27] “PAEKS Construction Based on LWE”- Ziqing Wang. - 2024

[28] “Efficient and Expressive Public Key Authenticated Encryption with Keyword Search in Multi-user Scenarios (v11)”- Jiayin Cai - 2025

[29] “Blockchain-based Privacy-Preserving Public Key Searchable Encryption (v12)”- Yue Han et al.- 2023

[30] “Public Key Authenticated Encryption with Keyword Search Improved (v14)” – Guiquan Yang -2024

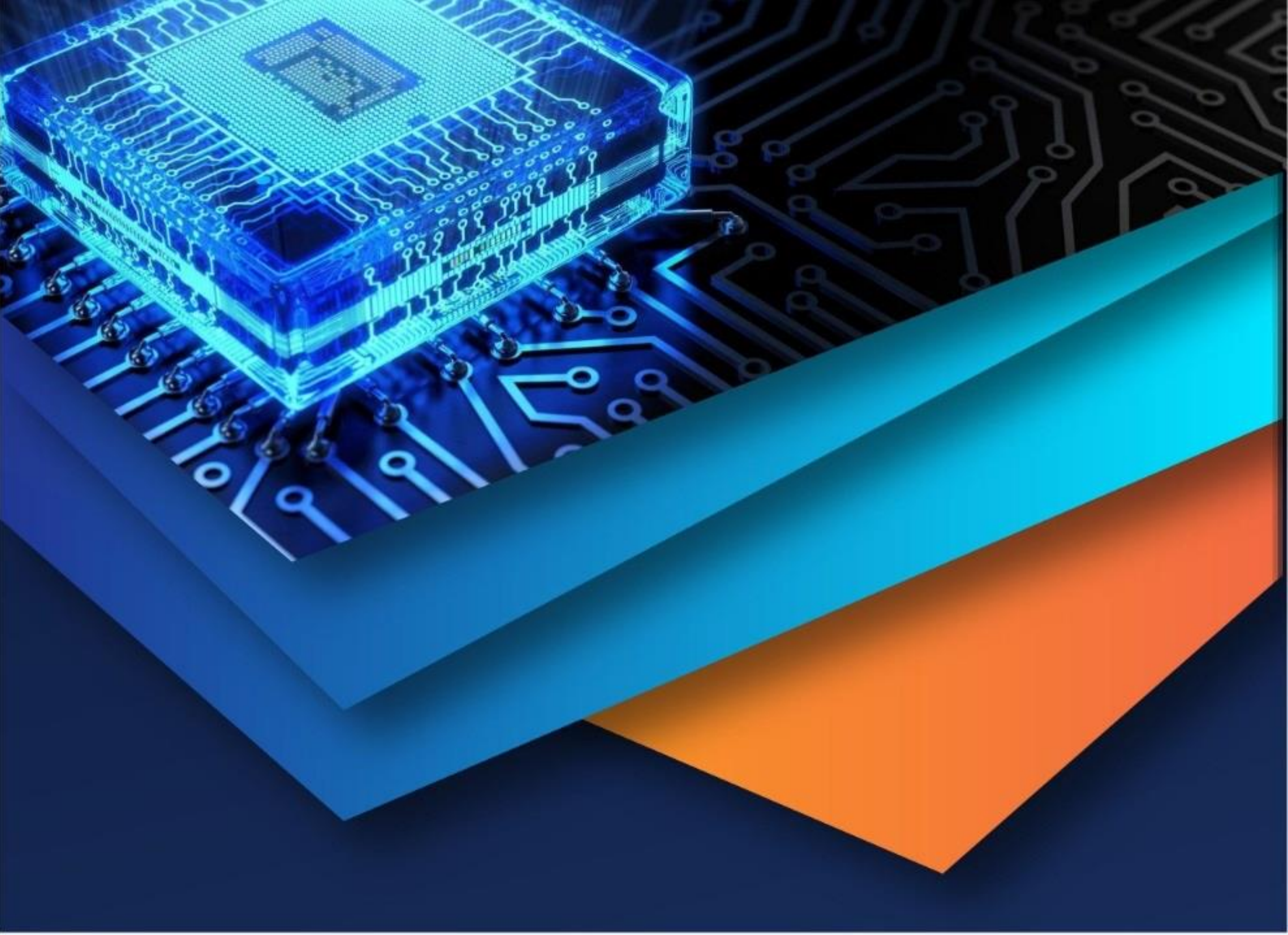
[31] “Hierarchical Identity-Based Authenticated Encryption (v15)” –Dorsa Shiraly et al.- 2024

[32] “Query-Recovery Attack on Searchable Encryption (v17)” – Marc Damie – 2023

[33] “Key-Updatable PEKS with Ciphertext Sharing (v18)” – Fen Wang et al.– 2022

[34] “PAEKS Construction Based on LWE (v19)” –Ziqing Wang – 2024

[35] “Survey on PEKS in Cloud (v20)” – Zhang – 2023



crossref
10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL
IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY