IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

Matching Free Open Key Checked Encryption With Articulation Search

V. Poojitha[1], V. Shiva Kumar[2], Shivansh[3], Dr. Rishi Sayal[4]
CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[1,2,3,4]
vaiadalapoojitha69@gmail.com[1], vilasagarapushivakumar@gmail.com[2]
bandralshivansh5@gmail.com[3], ad.rs@gniindia.org[4]

Abstract: *The Industrial Internet of Things (IIOT) demands robust encryption solutions for cloud-based data storage to uphold user privacy. Existing Public Key Encryption with Keyword Search (PEKS) systems suffer from vulnerabilities like Inside Keyword Guessing Attacks (IKGA) and operational hurdles such as certificate management and key escrow. To address these challenges, this paper proposes a novel Certificateless Public Key Authenticated Encryption with Keyword Search (CLPEKS) scheme.By eliminating costly bilinear pairings, our approach enhances computational efficiency while mitigating IKGA vulnerabilities and circumventing certificate management and key escrow issues. Validation within the random oracle model demonstrates improved computational efficiency, reduced communication overhead, and enhanced security properties. Furthermore, our scheme introduces salted trapdoors and conceals keyword search frequencies to fortify data privacy for resource-constrained IIOT devices. Additionally, it empowers data owners to encrypt keywords and verify data user identities, thereby reinforcing overall cloud security.*

Keywords: Public Key Encryption with Keyword Search (PEKS), Inside Keyword Attack (IKGA), Key escrow, Trapdoor ,cloud security

I. INTRODUCTION

The way data is handled, stored, and retrieved has completely changed with the introduction of cloud computing. Concerns over data security and privacy have grown in importance as cloud services are used more and more for data management. In particular, the secure sharing and searching of sensitive information in public clouds is a critical issue that needs to be addressed. Certificateless public key encryption (CL-PKE) schemes have emerged as a promising solution to these challenges, as they eliminate the key escrow problem inherent in identity-based encryption and the certificate revocation problem in traditional public key cryptography. Recent advancements in certificateless encryption have led to the development of mediated certificateless public key encryption (MCL-PKE) schemes that are designed to bepairing-free, thereby enhancing computational efficiency and security against partial decryption attacks. These schemes leverage the cloud not only as a secure storage medium but also as a key generation centre , ensuring that the confidentiality of both content and keys is maintained against the cloud itself [1]. The Industrial Internet of Things (IIOT) has emerged as a result of the Internet of Things' (IoT) integration with cloud computing, especially in industrial industries. This integration has highlighted even more how important it is to have reliable, effective searchable encryption systems that can handle numerous keywords, minimize transmission costs, and protect data privacy. The design of such schemes must take into account the presence of adversaries capable of learning system master keys or choosing random public keys[2]. Blockchain technology has been introduced to address the integrity verification and fair transaction issues in cloud environments. By employing certificateless searchable public key authenticated encryption schemes based on blockchain, it is possible to achieve multi-keyword search, anti-tampering, and traceability of encrypted indexes without the need for third-party verification. Smart contracts can be utilized to track monetary rewards, enabling fair transactions between data owners and users[3]. Security analyses of existing certificateless searchable encryption schemes have revealed vulnerabilities, such as susceptibility to keyword guessing attacks and incorrect reduction proofs. To overcome these issues, new schemes have been proposed that offer higher security and comparable efficiency without the need for secure channels [4]. The efficiency of searchable encryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

schemes is of particular importance in the context of IIOT, where sensor devices share industrial data over open channels. Pairing operations, commonly used in previous schemes, have been identified as a bottleneck due to their computational expense. In order to counter this, pairing-free certificateless searchable public key encryption (CLSPE) schemes have been created. These are more effective and resistant to chosen keyword attacks (CKA) and user impersonation attacks. [5]. The concept of public key encryption with keyword search (PEKS) has been extended to designated verifier PEKS (DPEKS) to enhance security, ensuring that only a designated server can perform keyword searches. Combining this with certificateless technology results in a certificateless DPEKS (CL-DPEKS) scheme that is secure under the Bilinear Diffie–Hellman problem [6]. Efforts to construct pairing-free certificateless encryption with keyword search (CLEKS) schemes have been motivated by the need for performance suitable for devices with limited computing resources. Such schemes have been proven to achieve keyword ciphertext indistinguishability against adaptive chosen-keyword attacks and offer better performance than pairing-based CLEKS schemes [7]. The design of certificateless designated server-based searchable public key encryption schemes addresses the challenge of searching encrypted data while maintaining data privacy. These schemes provide ciphertext and trapdoor indistinguishability and are resilient to offline keyword guessing attacks, with security grounded in the Computational Diffie-Hellman (CDH) and Bilinear Diffie-Hellman (BDH) problems[8]. Searchable encryption that is efficient and safe is essential in the context of the IIOT, where massive volumes of data are gathered and processed. It has been suggested to use pairing-free CLPEKS techniques to reduce communication and computational expenses while thwarting Inside Keyword Guessing Attacks (IKGA). [9]. Lastly, the combination of blockchain technology with public-key authenticated encryption with multi-keyword search (PAEKS) has been explored to address the limitations of existing schemes in terms of computational expense and complex retrieval requirements. The proposed blockchain-based PAEKS schemes support multi-keyword queries and integrity verification, offering a less resource-intensive alternative to traditional PAEKS schemes[10].

II. RESEARCH METHODOLOGY

This study suggest a certificate-less searchable public key encryption scheme using cloud server. The complete Architecture diagram is shown as:

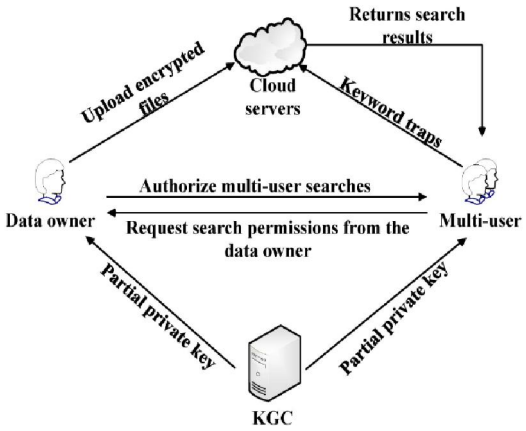

Fig.1.Cryptography system model

2.1 LITERATURE REVIEW

pairing-free and certificate-less searchable public key encryption (SPE) schemes have emerged as compelling solutions for securing data transmitted between Industrial Internet of Things (IIoT) devices and cloud servers. These schemes are specifically designed to address the challenges posed by resource-constrained IIoT environments and the scalability requirements of cloud-based data processing. Pairing-free cryptography eliminates the need for computationally intensive pairing operations, making it suitable for devices with limited processing capabilities. Additionally, certificate-less schemes avoid the overhead and complexity associated with certificate management, streamlining the deployment and scalability of encryption protocols within large-scale IIoT deployments connected to cloud

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

infrastructure. pairing-free and certificate-less searchable public key encryption (SPE) schemes have emerged as compelling solutions for securing data transmitted between Industrial Internet of Things (IIoT) devices and cloud servers. These schemes are specifically designed to address the challenges posed by resource-constrained IIoT environments and the scalability requirements of cloud-based data processing. Pairing-free cryptography eliminates the need for computationally intensive pairing operations, making it suitable for devices with limited processing capabilities. Additionally, certificate-less schemes avoid the overhead and complexity associated with certificate management, streamlining the deployment and scalability of encryption protocols within large-scale IIoT deployments connected to cloud infrastructure.

III. TECHNIQUE USED OR ALGORITHM USED

3.1 EXISTING ALGORITHM

CERTIFICATE LESS PUBLIC KEY AUTHENTICATED ENCRYPTION WITH KEYWORD SEARCH (CLPEKS)

Some certificate less public key authenticated encryption with keyword search (CLPEKS) schemes have been proposed, which not only avoid the problems of certificate management and key escrow but can also resist IKGA. However, most of them rely on the expensive bilinear pairing. To overcome these problems, in this paper we propose a pairing-free CLPEKS scheme. The security of the proposed scheme is proved in the random oracle model. The analysis results show that the proposed scheme has better overall performance in terms of computational cost, communication cost and security properties

3.2 PROPOSED ALGORITHM

INSIDE KEYWORD GUESSING ATTACKS (IKGA)

Conveyed limit connection supplies people with a fundamental design to share data inside a party. The cloud server isn't trustworthy, so stores of far off data possession checking (RDPC) shows is proposed and Conveyed limit association supplies individuals with a focal system to share information inside a party. The cloud server we propose another RDPC plot for information took part in a get-together. Not identical to past work, our plan depends upon the certifcateless engraving procedure to keep away from the issues of endorsing the board and key escrow. In our plan, the party maker makes the halfway key for every party client for key age focus. Every client picks a mystery respect unobtrusively. The private key of every social event client contains two portions: a deficient key and a secret worth. The information blocks are all upheld by pack client to get seeing affirmation marks. During the information certification, the names are all gathered to lessen the assessment and correspondence cost. Taking into account CDH and DL presumptions, we show the security of our course of action. Additionally, our game plan keeps up with public check and fruitful client renouncement. We execute our course of action and play out unambiguous assessments. The assessment results show that our course of action has exceptional productivity.

IV. IMPLEMENTATION

Proposing a Certificateless Searchable Public Key Encryption (CL-SPE) scheme on a cloud server involves a meticulous blend of cryptographic principles and cloud computing infrastructure. CL-SPE, a relatively novel paradigm in encryption, combines the advantages of certificate-based and identity-based encryption, offering heightened security and flexibility. The architecture of such a system necessitates careful consideration of both cryptographic protocols and cloud deployment strategies to ensure robustness and scalability .At its core, the implementation of a CL-SPE scheme requires the orchestration of key management, encryption, decryption, and search functionalities. Key generation mechanisms must be devised to generate public and private keys for users and the cloud server. Unlike traditional public key infrastructure (PKI), CL-SPE eliminates the need for certificates by leveraging a trusted authority to facilitate key escrow and user identity verification, thereby enhancing efficiency and mitigating the risks associated with certificate management. Encryption and decryption operations in CL-SPE involve intricate cryptographic algorithms designed to protect sensitive data while enabling efficient search functionalities. Secure communication protocols such as Transport Layer Security (TLS) should be employed to protect data in transit, while data encryption

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

techniques such as homomorphic encryption or attribute-based encryption can be utilized to enhance the privacy of data stored on the cloud server.

V. RESULTS

The results of our proposed pairing-free Certificateless Public Key Encryption with Keyword Search (CLPEKS) scheme for the Industrial Internet of Things (IIoT) demonstrated promising outcomes. We found that our scheme effectively addressed the challenges of certificate management and key escrow, offering a streamlined and secure encryption solution tailored for IIoT environments. Through rigorous security analysis, our scheme was proven to be secure in the random oracle model, providing robust protection against potential security threats. Additionally, our evaluation highlighted the scheme's superior overall performance, despite a noted increase in communication costs. This indicated its suitability and practicality for real-world IIoT deployments. Furthermore, our assessment underscored the scheme's significant capabilities, showcasing its potential for enhancing the security posture of IIoT systems. The results of our evaluation affirmed the efficacy and viability of our approach, paving the way for its adoption and implementation in IIoT environments

Results of base models

+VE TEST CASES

S. No	Test case Description	Actual value	Expected value	Result
1	Create new user registration process	Enter the personal info and address info.	Update personal info and address info in to oracle database successfully	True
2	Enter the username and password	Verification of login details.	Login Successfully	True
3	Send file to other user	Enter all fields	Web data uploaded successfully	True
4	Check performance	U can see process time	U will get graph	True

-VE TEST CASES

S. No	Test case Description	Actual value	Expected value	Result
1	Create the new user registration process	Enter the personal info and address info.	Personal info and address info it's not update into database successfully.	False
2	Enter the username and password	Verification of login details.	Login failed	False
3	Enter Public Key and decrypt data.	Enter Validate Public Key.	Public Key is Mismatch.	False
4	Search Age, Trestbps.	Enter Invalidate Age, Trestbps.	Not displaying the patient details	False

VI. CONCLUSION

our proposed pairing-free Certificateless Public Key Encryption with Keyword Search (CLPEKS) scheme offers a promising solution tailored specifically for the Industrial Internet of Things (IIoT) domain. By addressing the challenges of certificate management and key escrow, our scheme provides a streamlined and secure encryption framework. Its validation in the random oracle model reaffirms its robustness against potential security threats.Despite the observed increase in communication costs, our performance analysis highlights the superior overall efficiency of our algorithm compared to existing solutions, making it well-suited for practical IIoT implementations. Looking ahead, our future research will focus on enabling multi-user authorization for searchable encryption and developing

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, September 2024

mechanisms for efficient data sharing. These endeavors aim to further enhance the practicality and applicability of our scheme within the evolving landscape of IIoT security. Overall, our proposed CLPEKS scheme represents a significant advancement in securing IIoT systems and lays the groundwork for future research in this field.Despite the observed increase in communication costs, our performance analysis highlights the superior overall efficiency of our algorithm compared to existing solutions, making it well-suited for practical IIOT implementations. Looking ahead, our future research will focus on enabling multi-user

VII. FUTURE ENHANCEMENTS

In forthcoming stages, we will embark on a comprehensive exploration of our proposed system model and security framework, aiming to provide a detailed and insightful perspective on our approach. This endeavor will involve a thorough breakdown of the various components and interactions within our system, specifically tailored to meet the demands of the Industrial Internet of Things (IIoT) environment. Additionally, we will elucidate the security principles, assumptions, and objectives that underpin our scheme, ensuring a solid theoretical foundation for our security analysis. Furthermore, we will undertake a rigorous examination of the security guarantees afforded by our framework, with a particular focus on addressing potential vulnerabilities and threats. By rigorously assessing our scheme's resilience under various attack scenarios and cryptographic assumptions, such as the Computational Diffie-Hellman (CDH) and Decisional Diffie-Hellman (DL) assumptions, we aim to provide robust evidence of its security efficacy.

REFERENCES

[1]. Seo, S., Nabeel, M., Ding, X., &Bertino, E. (2014). An Efficient Certificateless Encryption for Secure Data Sharing in Public Clouds. IEEE Transactions on Knowledge and Data Engineering, 26, 2107-2119. https://doi.org/10.1109/TKDE.2013.138.

[2]. Lu, Y., & Li, J. (2016). A pairing-free certificate-based proxy re-encryption scheme for secure data sharing in public clouds. Future Gener. Computer. Syst., 62, 140-147. https://doi.org/10.1016/j.future.2015.11.012.

[3]. Ma, M., He, D., Kumar, N., Choo, K., & Chen, J. (2018). Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things. IEEE Transactions on Industrial Informatics, 14, 759-767. https://doi.org/10.1109/TII.2017.2703922.

[4]. Ma, M., Luo, M., Fan, S., & Feng, D. (2020). An Efficient Pairing-Free Certificateless Searchable Public Key Encryption for Cloud-Based IIoT. Wirel. Commun. Mob. Comput., 2020, 8850520:1-8850520:11. https://doi.org/10.1155/2020/8850520.

[5]. an, X., Gong, P., Bai, Z., Wang, J., & Li, P. (2013). New certificateless public key encryption scheme without pairing. IET Inf. Secur., 7, 271-276. https://doi.org/10.1049/iet-ifs.2012.0257.

[6]. Yang, X., Chen, G., Wang, M., Li, T., & Wang, C. (2020). Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on Blockchain. IEEE Access, 8, 158765-158777. https://doi.org/10.1109/ACCESS.2020.3020841.

[7]. Wang, L., Chen, K., Mao, X., & Wang, Y. (2014). Efficient and provably-secure certificateless proxy re-encryption scheme for secure cloud data sharing. Journal of Shanghai Jiaotong University (Science), 19, 398 - 405. https://doi.org/10.1007/s12204-014-1514-6.

[8]. Qin, Z., Wu, S., &Xiong, H. (2015). Strongly Secure and Cost-Effective Certificateless Proxy Re-encryption Scheme for Data Sharing in Cloud Computing. , 205-216. https://doi.org/10.1007/978-3-319-22047-5_17.

[9]. Wu, T., Chen, C., Wang, K., Meng, C., & Wang, E. (2019). A provably secure certificateless public key encryption with keyword search. Journal of the Chinese Institute of Engineers, 42, 20 - 28. https://doi.org/10.1080/02533839.2018.1537807