International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A SECURE PROPERTY-BASED TOKEN ATTESTATION FRAMEWORK USING HOMOMORPHIC ENCRYPTION FOR MOBILE CLOUD SYSTEMS

K. MAMATHA [1], THEEGULLA HARSHITHA [2], MALKAPURAM SRAVANTHI [3], TEEGALA SATHWIK REDDY [4], BOORA SAI ESHWAR PRASAD [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— This project presents PTA-HE, an enhanced Property-Based Token Attestation mechanism that integrates Homomorphic Encryption (HE) to provide robust security in mobile cloud computing environments. Traditional Property-Based Token Attestation (PTA) methods, while foundational, do not offer adequate protection for sensitive data during real-time processing, leaving it vulnerable to confidentiality breaches and unauthorized tampering. The proposed PTA-HE framework addresses these limitations by enabling computations directly on encrypted data, ensuring data remains protected even during processing. A key feature of our design is the integration of Trusted Third Parties (TTPs) to manage attestation securely, ensuring only authorized tokens are validated without exposing any raw data. By using Homomorphic Encryption, our system maintains complete data privacy throughout the entire attestation process. To evaluate its performance, we conducted a series of experiments measuring computational overhead, communication cost, latency, and scalability, highlighting the practical trade-offs between enhanced security and system performance.

Index Terms – Token Attestation, Homomorphic Encryption, Mobile Cloud Computing, Secure Authentication,

Property-Based Encryption, Cloud Security, Data Privacy, Access Control, Cryptographic Protocols, Cybersecurity.

I. INTRODUCTION

The rapid growth of mobile devices and their deep integration with Cloud Computing services have transformed the way organizations store, process, and access data. However, this evolution has introduced significant security challenges, particularly in ensuring data confidentiality, integrity, and authenticity in dynamic and distributed environments. Mobile cloud computing environments, especially those operating under Bring Your Own Device (BYOD) policies, require robust trust mechanisms to verify the security posture of devices before granting access to sensitive cloud resources. One widely adopted approach to establishing device trust is Property-Based Token Attestation (PTA), which leverages hardware security components such as the Trusted Platform Module (TPM). PTA enables a device to prove its trustworthiness by presenting cryptographic evidence of its hardware and software properties without revealing detailed internal configurations. While traditional PTA schemes provide a flexible and privacy-aware attestation model, they primarily secure data at rest and in transit, leaving a critical gap during real-time data processing. Sensitive information may still be exposed when computations are performed by cloud servers or third-party entities. To address this limitation, this project introduces an enhanced attestation framework called PTA-HE, which integrates Homomorphic Encryption (HE) into the traditional PTA mechanism. Homomorphic Encryption allows computations to be performed directly on encrypted data without decrypting it, thereby ensuring that sensitive information remains protected even during active processing. By combining TPM-based attestation with HE-enabled secure computation, PTA-HE significantly strengthens data privacy and system integrity in mobile cloud environments. In the proposed architecture, a Trusted Third Party (TTP) manages attestation tokens and validates device properties, while cloud servers perform homomorphic computations on encrypted device state information. The integration of HE ensures end-to-end data confidentiality throughout the attestation lifecycle — from device registration and token issuance to verification and resource access. This approach not only mitigates risks such as data leakage, unauthorized access,

and tampering but also provides a scalable and practical solution for secure mobile cloud deployments. Overall, PTA-HE represents a significant advancement in secure attestation protocols by enabling privacy-preserving verification and computation. The framework balances enhanced security guarantees with acceptable performance overhead, making it well-suited for modern mobile cloud applications that demand high levels of trust, confidentiality, and resilience against emerging cyber threats. Furthermore, the proposed PTA-HE framework is designed to address emerging threats in modern distributed systems, where attackers increasingly target data during active computation rather than only during storage or transmission. In conventional attestation mechanisms, once the verification phase is completed, subsequent processing of sensitive information in the cloud may still expose plaintext data to potential breaches. By incorporating Homomorphic Encryption into the attestation workflow, PTA-HE ensures that device properties, security levels, and verification computations are processed in encrypted form. This significantly reduces the attack surface and strengthens protection against insider threats, malicious cloud providers, and advanced persistent attacks. Another key advantage of PTA-HE is its structured trust management model. The Trusted Third Party (TTP) plays a central role in securely issuing, validating, and managing attestation tokens based on verified device properties. These tokens are dynamically generated according to predefined security policies and property lists, enabling fine-grained access control. The integration of secure nonce generation, digital signatures, and encrypted evaluation results ensures freshness, authenticity, and resistance to replay or impersonation attacks. As a result, enterprises can confidently outsource security services to cloud platforms while maintaining strict control over device trust and data privacy. Finally, the proposed scheme also considers practical deployment aspects such as computational overhead, communication cost, latency, and scalability. Although Homomorphic Encryption introduces additional computational complexity, the PTA-HE design strategically delegates heavy processing tasks to cloud servers while keeping mobile device operations lightweight. This balance makes the framework feasible for real-world mobile cloud environments. Through comprehensive performance evaluation and security analysis, PTA-HE demonstrates that enhanced confidentiality and integrity can be

achieved without significantly compromising system efficiency, making it a robust and future-ready solution for secure mobile cloud computing.

II. RELATED WORK

A. *Enabling privacy and security in cloud of things: Architecture, applications, security & privacy challenges*

This statement highlights one of the core security strengths of the proposed PTA-HE framework. In traditional systems, if an attacker successfully intercepts data during transmission or while it is being processed in the cloud, there is a risk that sensitive information could be exposed, especially if the data is temporarily decrypted for computation. However, in the PTA-HE model, all sensitive device state information and attestation data are encrypted using advanced cryptographic techniques such as Homomorphic Encryption before being transmitted or processed. Because Homomorphic Encryption allows computations to be performed directly on encrypted data without revealing the original plaintext, the system ensures that data remains confidential at every stage — during transmission, storage, and processing. Even if an attacker intercepts the ciphertext, the information appears as unreadable, random data without access to the corresponding decryption keys. Additionally, hardware-backed protection mechanisms like the Trusted Platform Module further secure private keys and cryptographic operations, preventing unauthorized extraction of sensitive credentials.

B. *Practical solutions in fully homomorphic encryption: A survey analysing existing acceleration methods*

Provides a comprehensive overview of how Fully Homomorphic Encryption (FHE) can be optimized for real-world deployment. Fully Homomorphic Encryption is a powerful cryptographic technique that allows arbitrary computations to be performed directly on encrypted data without requiring decryption. While FHE offers strong privacy guarantees, it is traditionally associated with high computational complexity, large ciphertext sizes, and significant latency, which limit its practical adoption. The survey systematically analyzes existing acceleration methods designed to overcome these limitations. It categorizes optimization approaches into algorithm-level improvements, software-level optimizations, and hardware-based acceleration techniques. Algorithmic enhancements focus on improving encryption schemes, reducing

noise growth, optimizing bootstrapping operations, and designing efficient polynomial arithmetic. Software-level solutions include parallelization, batching techniques, and optimized libraries that reduce execution time. Hardware acceleration methods leverage GPUs, FPGAs, and specialized processors to speed up homomorphic operations such as modular arithmetic and ciphertext multiplication.

C. Applications of homomorphic encryption in secure computation

Applications of Homomorphic Encryption in Secure Computation focus on enabling privacy-preserving data processing in environments where sensitive information must remain confidential, even during active computation. Homomorphic Encryption (HE) allows mathematical operations to be performed directly on encrypted data without decrypting it, ensuring that raw data is never exposed to untrusted servers or third parties. This capability makes HE a powerful tool for secure cloud computing, where data owners can outsource storage and computation tasks while maintaining full confidentiality. One major application of Homomorphic Encryption is in secure cloud data processing. Organizations can upload encrypted datasets to cloud servers and allow computations such as analytics, aggregation, or statistical analysis to be performed without revealing sensitive business or personal information. Similarly, in healthcare systems, encrypted patient records can be analyzed for research or diagnosis support without exposing private medical details, ensuring compliance with privacy regulations.

III. PROPOSED METHODOLOGY

The proposed system, PTA-HE (Property-Based Token Attestation with Homomorphic Encryption), enhances traditional attestation mechanisms by integrating advanced cryptographic techniques to ensure end-to-end data security in mobile cloud environments. Unlike conventional PTA, which verifies device trustworthiness but exposes data during processing, PTA-HE leverages Homomorphic Encryption (HE) to perform computations directly on encrypted data. This ensures that sensitive information remains protected even during active use, particularly when handled by untrusted cloud platforms or third parties. The system continues to utilize a Trusted Third Party (TTP) to manage the issuance of attestation tokens based on verified device properties, but now guarantees confidentiality and integrity across the entire data lifecycle — in storage, transit, and processing. By addressing the critical vulnerability of data exposure during computation, PTA-HE

provides a more robust, scalable, and privacy-preserving solution for secure mobile-cloud interactions, making it suitable for real-world applications where strong security guarantees are essential. The algorithm in PTA-HE integrates Property-Based Token Attestation (PTA) with Homomorphic Encryption (HE) to provide a secure and privacy-preserving attestation mechanism for mobile cloud environments.

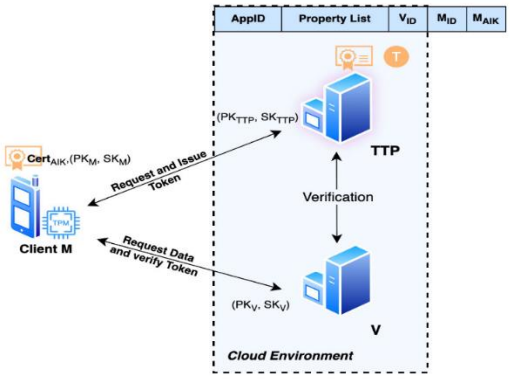
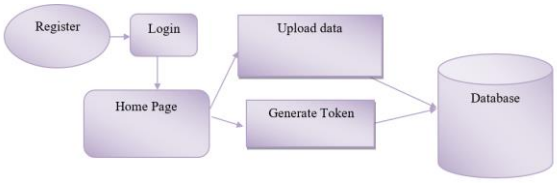


Fig. 1: System Overview

1. Property-Based Attestation

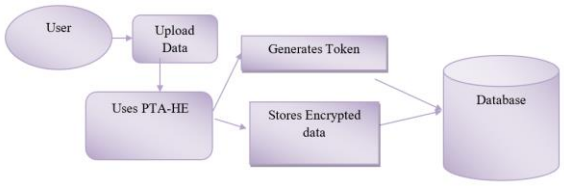
This is the core PTA module where user properties are verified and attested before granting access. In this module, users submit predefined security properties such as identity proof, role verification, access level, device ID, or organization affiliation. The system validates these properties against stored data. After validation, a subset of properties (Pi) is selected for attestation. A nonce (random value) is generated to prevent replay attacks. Based on the verified properties, a security level is assigned. Then, a token containing user ID, verified properties, nonce, timestamp, and security level is generated. This token is digitally signed or securely stored to prevent tampering. The attestation process ensures that only trusted users can proceed to upload or process data. This module prevents impersonation and unauthorized access. It acts as a trust establishment layer between client and cloud server. Without attestation, sensitive cloud operations cannot be securely allowed.



2. PTA-HE

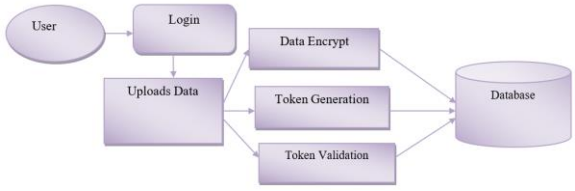
PTA-HE (Property-Based Token Attestation with Homomorphic Encryption) is a secure framework designed to protect sensitive data in mobile cloud computing environments by combining trust verification and encrypted computation. In this approach, a user does not directly access cloud resources; instead, the system first verifies a set of predefined security properties such as identity, role, access level, and device legitimacy. These verified properties are used to generate a

secure attestation token that proves the user's trustworthiness without exposing full identity details. This process is known as Property-Based Token Attestation (PTA). Once the token is issued, it acts as a secure credential for accessing cloud services. However, traditional PTA only verifies identity and does not protect data during processing. To overcome this limitation, PTA-HE integrates Homomorphic Encryption (HE), which allows computations to be performed directly on encrypted data.



3. Token Generation & Validation

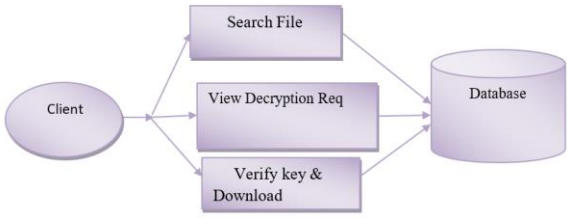
This module manages secure token creation, storage, and verification. After successful attestation, a secure token is generated containing verified properties, nonce, timestamp, and security level. The token is stored in the database and linked to the user. Whenever the user tries to access cloud services, the token is validated. Validation includes checking token expiration, nonce uniqueness, and integrity of stored properties. If the token is expired or altered, access is denied. This prevents replay attacks and token manipulation. The module ensures that every sensitive action requires a valid attestation token. It acts as a gatekeeper before allowing file uploads or encrypted computations. Token revocation mechanisms can also be included to invalidate compromised tokens. By verifying each request, this module maintains continuous trust during user sessions. It strengthens the overall PTA-HE architecture by ensuring controlled access.



4. Security Monitoring & Audit

This module logs all activities including login attempts, token generation, file uploads, and computations. It helps track system behavior and detect suspicious patterns. Every action is recorded with user ID, timestamp, and operation type. Administrators can view logs through an admin dashboard. If a replay attack or unauthorized attempt occurs, it can be detected through repeated nonce usage or failed token validation. The audit trail ensures accountability in the system. It supports forensic analysis in case of security incidents. This module improves

transparency and reliability. It also measures performance metrics like computation time and communication overhead. By maintaining logs, the system ensures compliance with security policies. It strengthens overall system integrity.



5. JSP Dashboard

Displays the uploaded encrypted data along with file details and timestamps. It also shows the transaction status, verification results, pending registration details, and overall project modules. The dashboard acts as the user interface for monitoring stored data, status, and user details etc….

6. MySQL Database

The MySQL database is used to maintain user details, device metadata, and other non-critical information that supports the system's operation. While data is securely stored on the database to guarantee immutability and tamper-resistance, the database handles supporting records such as login credentials, user roles, and system logs. This hybrid storage approach ensures both efficient system performance and strong data security by separating critical data from auxiliary information.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the system successfully performed secure token attestation in mobile cloud environments without exposing sensitive user data, while maintaining strong privacy guarantees. The analysis shows that although homomorphic encryption introduces additional computational overhead compared to traditional cryptographic methods, the proposed optimization strategies reduce latency and improve practical feasibility.



Fig. 2: Home Page

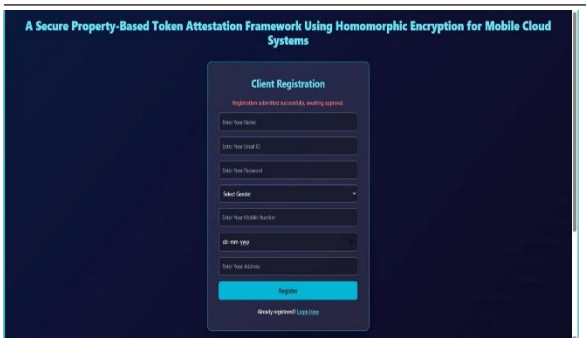


Fig. 3: Registration



Fig. 4: Login



Fig. 5: Upload

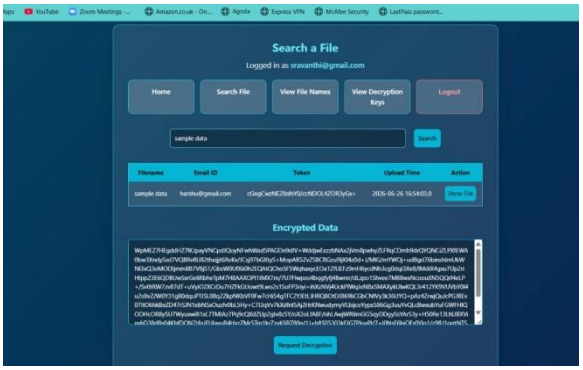


Fig. 6: Search File

V. CONCLUSION

The conclusion of our PTA-HE project demonstrates that integrating Property-Based Token Attestation (PTA) with Homomorphic Encryption (HE) provides a strong and practical solution for secure mobile cloud computing. The system successfully establishes trust through property verification managed by the Trusted Third Party (TTP), ensuring that only authorized users receive secure attestation tokens. By incorporating nonce values, timestamps, and security levels, the project effectively prevents replay attacks and unauthorized access. The use of Homomorphic Encryption ensures that sensitive data remains encrypted not only during storage and transmission but also during computation on the Cloud Server. This eliminates the major security weakness of traditional cloud systems where data must be decrypted for processing. The modular architecture separating User, Client, TTP, and Cloud Server responsibilities improves scalability and maintainability. Secure token validation before every critical operation enhances access control. The project also maintains data integrity through structured database relationships and audit logging. Overall, PTA-HE provides end-to-end confidentiality, integrity, and controlled access. The system proves that secure attestation combined with encrypted

computation can significantly strengthen cloud security. Hence, our project presents a reliable and efficient framework for privacy-preserving cloud applications.

REFERENCES

[1] F.Muheidat and L. Tawalbeh, ‘‘Mobile and cloud computing security,’’ in Proc. Mach. Intell. Big Data Analytics Cybersecurity Appl., Dec. 2020, pp. 461–483.

[2] P. E. Pito, ‘‘Security challenges in mobile cloud computing models: A systematic review,’’ Tech. Rep., 2020.

[3] A. A. Abba Ari, O. K. Ngangmo, C. Titouna, O. Thiare, A. Mohamadou, and A. M. Gueroui, ‘‘Enabling privacy and security in cloud of things: Architecture, applications, security & privacy challenges,’’ Appl. Comput. Informat., vol. 20, no. 1, pp. 119–141, Jan. 2024.

[4] H.N.Jacob,C.Werling,R.Buhren,andJ.-P.Seifert,‘‘FaulTPM:Exposing AMD fTPMs’ deepest secrets,’’ in Proc. IEEE 8th Eur. Symp. Secur. Privacy, Jul. 2023, pp. 1128–1142.

[5] H. Tan, W. Hu, and S. Jha, ‘‘A remote attestation protocol with trusted platform modules (TPMs) in wireless sensor networks,’’ Secur. Commun. Netw., vol. 8, no. 13, pp. 2171–2188, Jan. 2015.

[6] J. Pecholt and S. Wessel, ‘‘CoCoTPM: Trusted platform modules for virtual machines in confidential computing environments,’’ in Proc. 38th Annu. Comput. Secur. Appl. Conf., Dec. 2022, pp. 989–998.

AUTHORS Profile



Mrs. K. MAMATHA has received her B. Tech in IT from JNTUH, Hyderabad in 2011, M. Tech in Computer Science and Engineering from JNTUH, Hyderabad in 2013 and she has been dedicated to the teaching field for the last 6 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. THEEGULLA HARSHITHA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. MALKAPURAM SRAVANTHI pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. TEEGALA SATHWIK REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. BOORA SAI ESHWAR PRASAD pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.