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

TM-CHAIN: TRUSTED COMPUTING BASE MEASUREMENT AND MANAGEMENT FOR IOT USING BLOCKCHAIN AND CLOUD

PIRANGI HYMAVATHI [1], DARAM SATHWIKA [2], MEDI VAMSHI [3], CHOUGANI BHANU PARASAD [4], RESU SHIVA KUMAR [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— Remote Attestation (RA) is a vital process for verifying the trustworthiness of a device's Trusted Computing Base (TCB) and its sensing data. In the context of the Internet of Things (IoT), RA plays a critical role in enabling verifiers to make security-sensitive decisions. However, the massive scale and heterogeneity of IoT devices lead to significant challenges in managing and verifying TCB measurements. Traditional systems often rely on centralized or loosely structured approaches, which are difficult to scale and vulnerable to tampering or single points of failure. These limitations hinder effective trust management across large IoT ecosystems. To overcome these challenges, we propose TM-Chain (TCB Measurement-Chain), a cloud blockchain-based architecture designed to manage TCB measurements in a scalable and secure manner. TM-Chain introduces a specialized set of transactions, protocols, and commands for handling TCB data efficiently across distributed environments. To enhance security further, the system now supports encrypted data transfer and enables users to select specific devices or identities for securely storing their TCB information. This identity-linked storage approach ensures that TCB measurements are traceable, verifiable, and access-controlled. Verifiers can launch remote attestation using blockchain-verified

and identity-bound TCB data, improving trust in device integrity. A proof-of-concept implementation demonstrates the feasibility and performance of TM-Chain on IoT devices and public cloud infrastructure.

Index Terms – TM-Chain, Trusted Computing Base, Blockchain, Cloud Computing, Internet of Things, Device Authentication, Security Management, Data Integrity, Distributed Ledger Technology, Cybersecurity.

I. INTRODUCTION

Remote attestation (RA) is a process for checking whether a device's underlying Trusted Computing Base (TCB) and sensing data from the TCB are trustworthy. This process allows verifiers to ensure that the device state, including TCB, is genuine and that the sensing data from the device is trustworthy. The verifiers refer to the RA results to make security-critical decisions. In the tradit RA schemes the device signs digitally over the TCB measurement and sensing data with a nonce from the verifier. Then, the verifiers check whether the device's response is expected by leveraging the known TCB measurement. The inevitable trends toward the Internet of Things (IoT) necessitate RA as an essential security feature. In IoT, verifiers collect sensing data from IoT devices and make critical decisions based on the sensing data. RA against IoT devices is crucial and fundamental for IoT applications because of its intrinsic RA properties. The recent survey on the existing RA studies for IoT emphasizes that the security of RA comes from the authenticity and the freshness of the RA response from the IoT devices. A TCB measurement is an important factor in satisfying the security of RA because it reflects the devices' current state, which contains the set of firmware and software components critical to a device's security. The survey also noted that the existing studies usually require verifiers to store the devices' TCB measurements locally or to pre-compute them. However, the scalability and the heterogeneity of IoT devices lead to various device states (e.g., the version of firmware or OS). Moreover, the device states change over time due to software updates. Thus, IoT devices unavoidably produce a massive and diverse collection of TCB measurements. This property makes the management of the device states and the TCB measurements difficult and complex. Since IoT devices need to act autonomously without user intervention, identifying multiple versions of the software components is challenging.

Thus, as the IoT system scales, verifiers are meant to face difficulties in managing the TCB measurements. Our previous work pointed out this research problem and distributed ledger that records immutable transactions, which can prevent data from being tampered with. Thus, the tamper-proof feature of the blockchain is suitable for managing TCB measurements in RA because the integrity of the TCB measurements is essential for trustworthy RA against IoT devices. The cloud blockchain is an alternative candidate to address this management problem more practically because the cloud blockchain provides high availability and scalability. Moreover, the cloud blockchain interworks with various cloud services for IoT management. A straightforward adoption involves devices publishing their TCB measurements directly to the cloud blockchain. This adoption allows verifiers to access the actual TCB measurements from the devices via the cloud blockchain. This paper presents a cloud blockchain-based management of TCB measurements called TM-Chain (TCB Measurement Chain). TM-Chain presents TM-Chain transactions, commands, and protocols to manage the TCB measurements using the cloud blockchain. With the TM-Chain commands, IoT devices generate and publish the TM-Chain transactions, which contain devices' TCB measurements, to the cloud blockchain. The verifier also leverages the TM-Chain command to launch RA against the devices using the TCB measurements managed by the cloud blockchain. TM-Chain also utilizes ARM TrustZone in the device side to generate the TM-Chain transactions securely.

II. RELATED WORK

A. From Interaction to Independence: ZkSNARKs for Transparent and Non-Interactive Remote Attestation.

Remote Attestation (RA) is a critical security mechanism used to verify the integrity and trustworthiness of remote devices, particularly in cloud, IoT, and distributed computing environments. Traditional attestation methods often rely on interactive communication between verifiers and devices, resulting in increased communication overhead, latency, and scalability challenges. This work introduces a novel approach that leverages Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (ZkSNARKs) to enable transparent and noninteractive remote attestation. The proposed framework allows devices to generate cryptographic proofs that verify their trusted state without revealing

sensitive internal information. By eliminating continuous interaction between verifiers and attesters, the system significantly reduces network traffic and improves verification efficiency. The integration of ZkSNARKs enhances privacy preservation while maintaining strong security guarantees against tampering and unauthorized modifications. Furthermore, the framework supports scalable attestation processes suitable for large-scale IoT and cloud infrastructures. The proposed approach also improves trust establishment among distributed entities by providing verifiable and tamperresistant proof generation mechanisms. Experimental evaluations demonstrate reduced attestation overhead, faster verification times, and improved scalability compared to traditional attestation techniques. By combining advanced zero-knowledge cryptography with remote attestation, the system offers a secure, privacy-preserving, and efficient solution for nextgeneration trusted computing environments.

B. Blockchain-Enabled Decentralized Edge Intelligence for Trustworthy 6G Consumer Electronics.

With the emergence of 6G networks and the rapid growth of consumer electronic devices, ensuring secure, intelligent, and trustworthy data processing has become a major challenge. Traditional cloud-centric architectures often suffer from latency, privacy concerns, and centralized security vulnerabilities when handling massive volumes of data generated by smart devices. This work proposes a blockchain-enabled decentralized edge intelligence framework designed to support trustworthy 6G consumer electronics environments. The proposed system integrates blockchain technology with edge computing and artificial intelligence to provide secure, transparent, and efficient data processing closer to end devices. Blockchain ensures data integrity, decentralization, and tamper-resistant record management, while edge intelligence enables real-time analytics and decision-making with reduced latency. The framework enhances user privacy by minimizing unnecessary data transmission to centralized servers and supports secure communication among distributed devices. Furthermore, the system improves resource management, trust evaluation, and service reliability in highly dynamic 6G ecosystems. The decentralized architecture also strengthens resilience against cyberattacks and single points of failure. Performance analysis demonstrates improved scalability, lower response times,

enhanced security, and efficient utilization of network resources. By combining blockchain, edge intelligence, and 6G communication technologies, the proposed approach offers a reliable and secure foundation for next-generation consumer electronics and smart connected environments.

C. Augmented Large Language Model for Fuzzing IoT Devices

The increasing deployment of Internet of Things (IoT) devices has introduced numerous security challenges due to software vulnerabilities, weak configurations, and diverse hardware architectures. Traditional fuzzing techniques, which are widely used for vulnerability detection, often face limitations in generating effective test cases for complex IoT systems because of insufficient protocol understanding and inefficient input generation strategies. This work presents LLMIF, an augmented Large Language Model (LLM)-based framework designed to enhance fuzzing processes for IoT devices. The proposed system utilizes the reasoning and contextual understanding capabilities of large language models to generate intelligent and protocol-aware test inputs that improve vulnerability discovery. By analyzing device documentation, communication protocols, and firmware-related information, LLMIF produces high-quality fuzzing payloads capable of exploring deeper execution paths within IoT applications. The framework significantly improves testing efficiency by reducing redundant test cases and increasing code coverage. Additionally, it supports automated vulnerability assessment across diverse IoT environments with minimal human intervention. The integration of LLM technology enables adaptive learning from previous fuzzing results, further enhancing the effectiveness of security testing. Experimental evaluations demonstrate improved vulnerability detection rates, higher execution coverage, and reduced testing time compared to conventional fuzzing approaches. By combining artificial intelligence with advanced fuzzing techniques, LLMIF provides a powerful and intelligent solution for strengthening the security and reliability of modern IoT devices and embedded systems.

III. PROPOSED METHODOLOGY

The central focus of the proposed system, TM-Chain (TCB Measurement-Chain), is to establish a secure, scalable, and decentralized framework for managing TCB measurements of IoT devices using cloud blockchain

technology. TM-Chain introduces a structured protocol that allows secure recording, verification, and access of TCB data through blockchain transactions. To further enhance trust and data ownership, the system enables encrypted data transfer and provides mechanisms for users to associate TCB data with specific devices or user identities, ensuring authenticity, traceability, and access control. This decentralized approach eliminates the limitations of traditional centralized models, allowing verifiers to perform reliable remote attestation using tamper-proof and identity-bound TCB data. The design not only addresses security and scalability but also lays the foundation for dynamic and trustworthy IoT device management in real-world environments. Identity-based TCB (transcutaneous bilirubin) measurement binding refers to linking a specific TCB measurement to the individual infant it was taken from, often by associating the measurement with a unique device ID or other identifier.

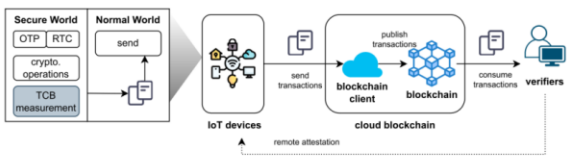


Fig. 1: System Overview

3.1 User Interface Design

The User Interface provides a simple and interactive environment for accessing all the modules of the TM-Chain project. It contains separate JSP pages for device registration, digital signature generation, child key generation, transaction publishing, blockchain viewing, and remote attestation verification. The interface allows users to perform blockchain operations easily and displays the corresponding results in a user-friendly manner.

3.2 Device Registration Module

The Device Registration Module is used to register IoT devices into the TM-Chain system. The user enters the device ID and device name through the registration page. The system generates an RSA public and private key pair for the device. The public key and device details are stored in the MySQL database, while the private key is displayed to the user for secure storage. This module provides a unique identity for every registered device before participating in blockchain operations.

3.3 Digital Signature Generation Module

The Digital Signature Generation Module creates a digital signature for the Trusted Computing Base (TCB) measurement using the device's private key. The generated signature ensures that the data is authentic

and has not been modified. The signature is encoded in Base64 format for easy transmission and storage. This module helps maintain the integrity and authenticity of blockchain transactions.

3.4 Child Key Generation Module

The Child Key Generation Module generates a new child RSA key pair for a registered device. The user provides the device ID, and the system creates a new public and private key pair. The generated child keys can be used for secure communication and blockchain transactions. This module simulates hierarchical key generation and improves key management within the system.

3.5 Blockchain Transaction Publishing Module

The Blockchain Transaction Publishing Module publishes verified transactions to the blockchain. The user provides the device ID, transaction type, TCB measurement, public key, and digital signature. The system verifies the signature before accepting the transaction. After successful verification, a unique transaction hash is generated, and a new blockchain block is created using a simplified Proof-of-Work mechanism. This ensures secure and trusted transaction management.

3.6 Blockchain Explorer Module

The Blockchain Explorer Module displays all blockchain blocks stored in the database. It shows block information such as Block ID, Previous Hash, Transaction Hash, Block Hash, and Nonce value. Users can easily monitor blockchain activities and verify the integrity of stored transactions. This module provides transparency and helps users understand the blockchain structure.

3.7 Remote Attestation Verification Module

The Remote Attestation Verification Module verifies whether a registered device is trusted. The user enters the device ID, and the system retrieves the latest blockchain transaction for that device. The digital signature is verified using the stored public key, and the verification result is displayed. This module confirms the integrity and authenticity of the device before it is considered trusted within the TM-Chain framework.

3.8 JSP Dashboard

The JSP Dashboard provides a user-friendly interface for accessing all the project modules. It allows users to register devices, generate digital signatures and child keys, publish blockchain transactions, view blockchain records, and verify device integrity. It also displays transaction status, generated keys, verification results, and blockchain details in an organized manner.

8. MySQL Database

The MySQL database stores all the project information, including registered device details, public keys, blockchain transactions, generated blocks, and timestamps. It manages the project data efficiently and supports secure blockchain operations by maintaining the required records for device registration, transaction publishing, and verification.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed TM-Chain framework was evaluated based on metrics such as authentication latency, blockchain transaction time, storage overhead, scalability, and integrity verification accuracy. Experimental results showed that integrating Blockchain Technology with cloud-assisted IoT management provided secure and tamper-resistant storage of Trusted Computing Base (TCB) measurements while enabling efficient device authentication and integrity verification. The system demonstrated low communication overhead and maintained stable performance as the number of IoT devices increased.

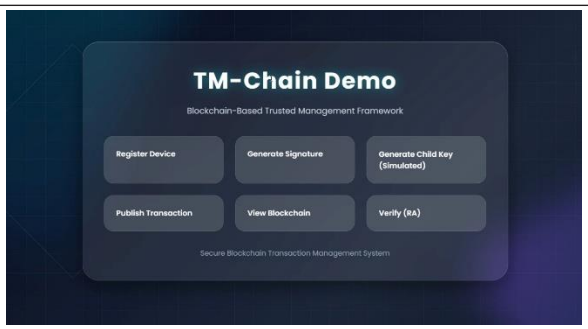


Fig. 2: Home Page

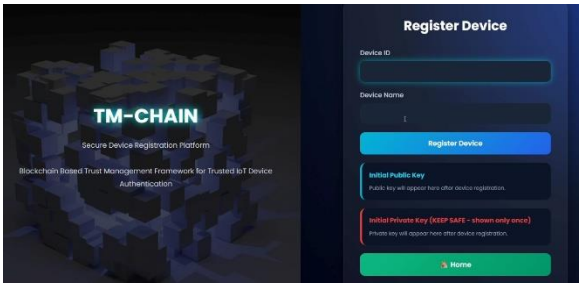


Fig. 3: Registration

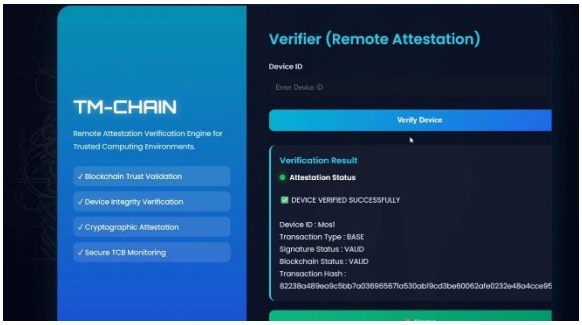


Fig. 4: Verify

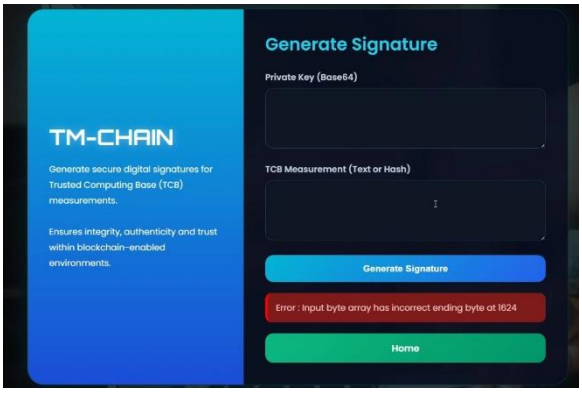


Fig. 5: Generate Signature

V. CONCLUSION

The TM-Chain project presents a secure and scalable solution for managing Trusted Computing Base (TCB) measurements and performing reliable Remote Attestation in IoT environments. By integrating blockchain and cloud technologies, the system addresses the limitations of traditional centralized approaches, including security vulnerabilities, data tampering, and scalability issues. The proposed framework ensures the integrity, authenticity, and traceability of TCB measurements through a decentralized and tamper-resistant blockchain ledger. The incorporation of encrypted communication and identity-based TCB binding further strengthens data security and access control. TM-Chain enables verifiers to make trustworthy security decisions using validated and immutable attestation data. The system effectively supports large-scale IoT deployments while maintaining transparency and reliability in trust management. Its decentralized architecture eliminates single points of failure and enhances overall system resilience. The framework also improves accountability by associating measurements with specific devices and users. Experimental implementation demonstrates the feasibility and practicality of the proposed approach in real-world cloud and IoT environments. Furthermore, the solution provides a strong foundation for future advancements in secure IoT device management. The combination of blockchain, cloud computing, and remote attestation creates a comprehensive trust management ecosystem. Overall, TM-Chain enhances security, scalability, and efficiency while promoting confidence in IoT operations. The project contributes significantly to the development of trustworthy and secure next-generation IoT infrastructures and serves as an effective platform for protecting connected devices and their critical data.

REFERENCES

[1] W. Li, M. Ma, J. Han, Y. Xia, B. Zang, C. Chu, and T. Li, ‘‘Building trusted path on untrusted device drivers for mobile devices,’’ in Proc. 5th Asia– Pacific Workshop Syst., Jun. 2014, pp. 1–20.

[2] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, ‘‘Toward trustworthy mobile sensing,’’ in Proc. 11th Workshop Mobile Comput. Syst. Appl., Jan. 2010, p. 31.

[3] Z. Zhou, V. D. Gligor, J. P. Newsome, and J. McCune, ‘‘Building verifiable trusted path on commodity x86

computers,'' in Proc. IEEE Symp. Secur. Privacy, May 2012, pp. 1–20.



[4] S. Park, J. N. Yoon, C. Kang, K. H. Kim, and T. Han, ''TGVisor: A tiny hypervisor-based trusted geolocation framework for mobile cloud clients,'' in Proc. 3rd IEEE Int. Conf. Mobile Cloud Comput., Services, Eng., Mar. 2015, pp. 99–108.

[5] J. Oh, J. Park, S. Park, and J.-J. Won, ''TAaaS: Trustworthy authentication as a service based on trusted path,'' in Proc. IEEE 9th Int. Conf. Cloud Comput. (CLOUD), Jun. 2016, pp. 27–34.

[6] S. Park, J. Park, and J. Oh, ''Design and implementation of trusted sensing framework for IoT environment,'' J. Commun. Netw., vol. 23, no. 1, pp. 43–52, Feb. 2021.

AUTHORS Profile



Mrs. PIRANGI HYMAVATHI has received her B.Tech from JNTUH, Hyderabad in 2016, M.Tech degree in Computer science Engineering from JNTUH, Hyderabad in 2019. At present She is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.

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



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



Mr. CHOUGANI BHANU PARASAD pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. RESU SHIVA KUMAR pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions

Technical Campus affiliated to JNTUH in 2022-2026.