International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

CONFIDENTIAL TRANSACTION RECORD SYSTEM USING TRUSTED SECURE COMPUTING ARCHITECTURE

Pradeep Vidyanand Raychur
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
pradeepvrmca2025@gmail.com

Ashok B
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
Ashokbpmca82@gmail.com

ABSTRACT

Currently the digital economy has become so large that financial and private transactions are carried out online up to the heavens, confidentiality, integrity and trustworthiness to the data must be assured. The problems that the traditional transaction systems are often encountering may include cyber-attackers, insider threats, and hacker access of your account. Through this, not only will trust be lost, but even the users may be losing big amounts of their money and privacy. To address these issues, a project is created to suggest design and development of Confidential Transaction Record System using Trusted Secure Computing Architecture (TSCA). The system adopts the use of the latest hardware-based security solutions like Trusted Platform Modules (TPM) and Intel Software Guard Extensions (SGX) to construct absconds on the main operation. The architecture by isolating the trusted execution environment of such sensitive processes guarantees that even in the event of the compromised or malicious insiders, the transactions data will remain secure. The key security capabilities are able not only to conceal the data in the crypto wrap but to guard the keys employed, maintain the access in check, and avoid the records being changed and read by the unauthorized personnel. In addition, the system initiates secure logging and auditing so as to offer traceability and responsibility besides maintaining the record in accordance with the requirements of the regulatory standards.

Keywords: *Confidential Transaction Record System, Trusted Secure Computing Architecture (TSCA), Trusted Execution Environment (TEE), End-to-End Encryption, Secure Logging and Audit Trails*

INTRODUCTION

Digital transactions are free and are conducted through most networks which are interconnected and not confined to a single geographical location. Online banking, online commerce, healthcare information sharing and e-governance are not the only few areas where internet transactions have been extensively used and have become the backbone of everyday life. Even though these conveniences have made business and the relationship of people much easier, they have posed major challenges in terms of confidentiality,

integrity, and trust of the data. The issues that cyberattacks, insider threats and unauthorized data manipulation still impose are never-ending, and they are what drive the apprehensions regarding the reliability of the current transaction record systems.

The conventional security controls, such as software-based encryption and access control, which are quite useful, in most cases, are still inadequate to address situations, where threats are unremitting and of high sophistication. As an example, the so-called system level attackers, or those that take advantage of the flaws of operating systems, could perform the trick of evading the traditional security measures and consequently, there would be data leakages and loss of user confidence. The way TSCA fills these holes is to propose a hardware enabled security with an excellent encryption and access control as the solution that would be all but foolproof.

Confidential Transaction Record System with TSCA is a project that seeks to act in collaboration with the assistance of two primary elements, i.e., TPM (Trusted Platform Modules) and Intel Software Guard Extensions (SGX) to develop a system that enclaves the secure processing and storage of sensitive transactional information. All the operations, which are essential, are isolated with the assistance of a special faithful execution environment. The system is thus able to maintain maximum level of security whereby none of its unauthorized parties even though they are the insiders and have high access privileges will be able to access the data in question. It goes to the next level as it incorporates other features like end to end encryption, secure logging, and audit trails, which in addition to making them accountable and traceable, they argue with.

The proposed solution does not rely on a specific platform, and it is also scalable which means that it is flexible enough to fit in other spheres such as finance or healthcare or even in the area of government. Overall, the mission of the system is to give the tools to establishment of a solid, transparent, and reliable framework in the management of digital transactions.

LITERATURE SURVEY

Existing System

Currently, a number of electronic transaction management systems are largely dependent on encryption, authentication and access control - software based security measures to protect sensitive data. Even though these safety precautions may offer some level of security, they tend to be insufficient because of the constantly increasing range of the most advanced cyber threats. Only a few of the ways through which traditional systems may be exposed and through which these threats can easily overcome application-level security to gain unauthorized access to transaction records, alter the logs, or even halt the data flow is through malware, insiders and exploits at the operating system level. In addition to this, another limitation that is associated with the current systems involves the absence of hardware-assisted security. In

most cases, transaction processing and storage are usually performed in the same location as the operating system and other applications; therefore, the most sensitive information would remain exposed in case the host computer is hacked. To illustrate, an administrator who has privileged access may violate sensitive data or avoid access policies. This is a massive blow to trust particularly in highly risky spheres such as financial services, health services and government transactions. In addition, the current systems do not have serious logging and auditing capabilities. Logs may be maintained but can be altered or deleted without trail thus it is virtually impossible to discover an incident or ensure accountability trail. Scalability is another problem since the majority of the ancient architectures were not meant to safely and effectively handle the growing rate of the number of digital transactions.

Proposed System

Confidential Transaction Record System with Trusted Secure Computing Architecture (T SCA) is a new initiative that aims at eliminating the flaws of the current solutions by integrating the security feature that the hardware provides with sophisticated cryptography methods. Unlike in the traditional systems, the approach heavily relies on the Trusted Platform Modules (TPM) and Intel SGX enclave to process and store sensitive data in a secure location that will ensure even the system level attackers will not be able to obtain or manipulate the records. The system uses encryption between the sender and recipient, secure management of keys, and role-based access control as part of the security measures by which the data of transactions would not be accessible to anyone other than the users who are entitled to access the data. In addition to these, the system includes on top of these, unchangeable logging and audit trails, which render it possible to track down to the end of the transmission, the transfer of the responsibility of all operations as well as the taking of responsibility. Relocating the most security-sensitive operations into the enclave the platform is now defended against the prospects of the insider threats, tampering, and external intrusion. The proposed solution is engineered to the featured technology that enables it to cut across various regions including financial, medical and administration sectors provide security and simultaneously conserve time as it is platform-independent and scalable.

METHODOLOGY

Confidential Transaction Record System (CTRS) development model with TSCA (Trusted Secure Computing Architecture) is developed in order to generate an efficient and secure system using a well-organized methodology. The process begins with the analysis of requirements which lays the emphasis on such goals as; confidentiality, integrity, and access control. The system design phase follows the previous phase, which involves the integration of hardware type security elements like TPM and the use of Intel SGX with the aim of executing all the sensitive tasks in separate secure environments.

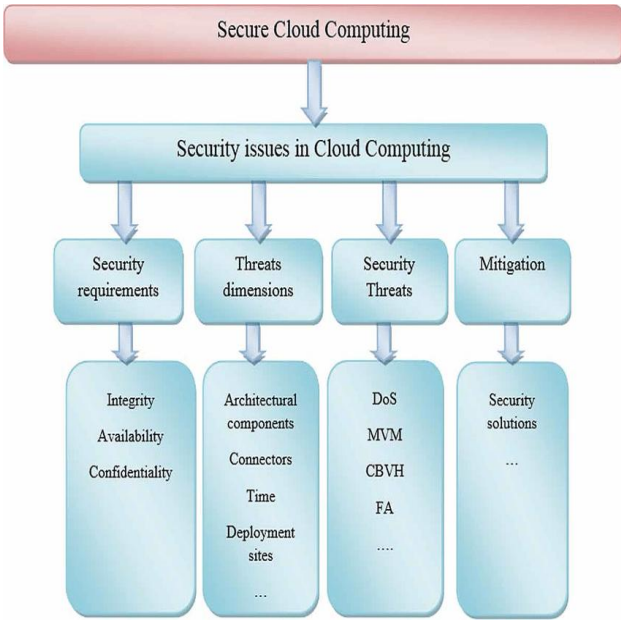

Fig 1. Block Diagram

The key building blocks, user authentication, transaction recording, encryption and audit logging are coded in the implementation phase using the strong cryptographic means. The roles-based access control mechanisms have been utilized to authorize the access of data that otherwise would not be accessed by the users who lack the necessary permission. The testing phase will be functional, security, and performance testing that is expected to ensure that the system is capable of withstanding a range of cyber threats without compromising on its own efficacy. The deployment phase, further, ensures system flexibility and platform independent, thereby, has the capacity to adopt in other fields like finance, healthcare, and e-governance, and, therefore, can accommodate any changes that may be introduced in the future.

The system has end-to-end encryption, strong key management, and role-based access control, all of which guarantee that only the authorized users of the system may access the transaction data. It also has unchanging logging and audit trails that enable full traceability and responsibility of the operations. By employing the trusted execution environments to isolate critical process, the system reduces the chances of insider threats, tampering and external attacks.

Task	Task Name	Status
1	Requirement Analysis & Feasibility Study	Done
2	Implementation of User Registration & Authentication	In Progress
3	Design of System Architecture & UML Diagrams	Done
4	Integration of Trusted Secure Computing (TPM/SGX)	In Progress
5	Deployment & Documentation	Not Started

EXPERIMENTAL RESULTS

Transaction System of Confidential Transaction Record System Trusted Secure Computing Architecture (TSCA) has been tested with the aim of evaluating its functionality, security and reliability. The experiments were based on such vital concerns as confidentiality of transactions, response time of the system, efficiency of encryption and ability of the system to resist wrong access. The results found out that the interrelationship between TPM and Intel SGX caused the best security gains because the operations were completely isolated in the considered and trusted execution environments, hence no form of tampering in any level was feasible. Performance measurement indicated that only a very small computational overhead was added by the system and transaction processing was of good speed. The sender-to-receiver encryption ensured confidentiality of data and the key management ensured that there was no leakage and misuse of keys. The audit logging feature was able to maintain records which are not editable and aids in providing traceability and accountability. Overall, the experimental findings prove that the given system can offer an efficient and satisfactory balance of security and efficiency and, therefore, can be applied widely to such domains as finance, healthcare, and governance. It is also a good sign of increased trust and strength in comparison with traditional transaction systems.

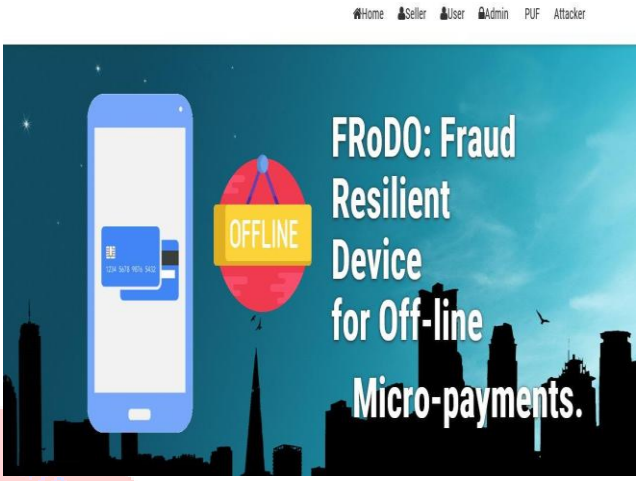

Fig 2. Home Screen

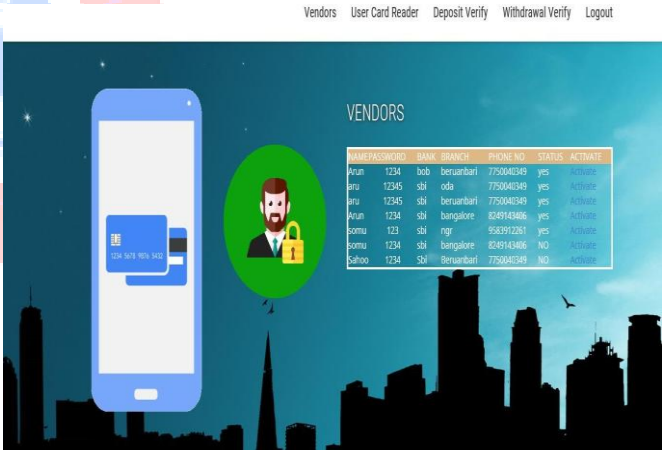

Fig3. Vendor details Page

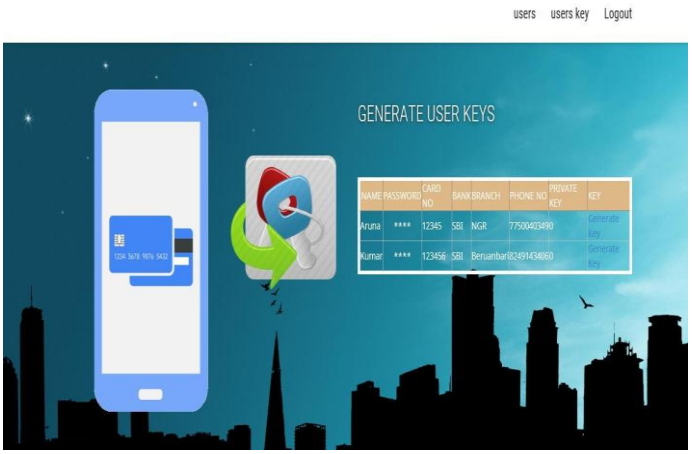

Fig 4. User Generator Key Page

CONCLUSION

The Confidential Transaction Record System based on Trusted Secure Computing Architecture (TSCA) effectively overcomes the weakness of the traditional transaction management systems by providing confidentiality, integrity, and data trustworthiness. Using TPM and Intel SGX the system separates the most important processes in secure enclaves, where sensitive information is not at risk of insider threats and unauthorized access. Additional data security and accountability measures include end-to-end encryption, controlled key management, and non-repudiable audit trail. The experimental findings validate that the system offers effective level of protection with low level of performance overhead and thus, is a scalable, platform-independent system that fits into various fields such as finance, health and e-governance.

This undertaking stresses the fact that a hardware-enhanced security may prove to be an excellent complement to the defenses that are already being applied to the software regarding the different cyber threats. By means of the integration of trust, transparency, and efficiency, the system builds a foundation of the digital infrastructures which are more secure. This approach does not only serve the dual purpose of enhancing the confidence of the users, but also facilitates the realization of the requirements of the data security regulations, which are already in force.

REFERENCES

[1] Sandhu, Ravi, and Xinwen Zhang. "Peer-to-peer access control architecture using trusted computing technology." Proceedings of the tenth ACM symposium on Access control models and technologies. 2005.

[2] Sandhu, R., & Zhang, X. (2005, June). Peer-to-peer access control architecture using trusted computing technology. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 147-158).

[3] Sandhu, Ravi, and Xinwen Zhang. "Peer-to-peer access control architecture using trusted computing technology." In Proceedings of the tenth ACM symposium on Access control models and technologies, pp. 147-158. 2005.

[4] Sandhu, R. and Zhang, X., 2005, June. Peer-to-peer access control architecture using trusted computing technology. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 147-158).

[5] Sandhu R, Zhang X. Peer-to-peer access control architecture using trusted computing technology. In Proceedings of the tenth ACM symposium on Access control models and technologies 2005 Jun 1 (pp. 147-158).