IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Exploring A Cryptographic Sollution In Blockchain For Privacy And Preserving Auction System

Mavilla Pavithra[1], Mr.A.J.Rajasekhar[2]

[1]PG student, Vemu Institute of Technology, P. Kothakota

[2]Associate professor, Vemu Institute of Technology, P. Kothakota

ABSTRACT

This paper addresses the privacy concerns in blockchain-based bidding systems, where bidding records, once stored, become immutable and visible only to the bidder and seller. However, this security measure falls short in cases of coercion, potentially compromising user privacy. To mitigate this, we introduce Deniable Matchmaking Encryption (DME), enhancing privacy by providing deniability for both messages and identities. Utilizing the chameleon hash function, our scheme ensures that fake messages and identities are indistinguishable from real ones. As an extension, our modified DME algorithm enables all bidders to decrypt and view the winning notification, safeguarding both the winner's identity and the transparency of the bidding process, thereby preserving user privacy while maintaining system integrity.

Keywords: blockchain, DME

INTRODUCTION

In the rapidly evolving landscape of commerce, blockchain technology has emerged as a transformative force, particularly enhancing the reliability and transparency of commercial applications. Its decentralized and immutable nature offers a solution to the age-old trust issue in bidding systems. Unlike traditional methods, where ensuring the secure and untampered delivery of bids is a challenge, blockchain-based systems ensure bid integrity and confidentiality between the buyer and seller. However, maintaining privacy and preventing coercion-induced breaches remain paramount. Traditional encryption schemes like matchmaking encryption (ME) offer anonymity but fall short against coercive threats. This paper introduces Deniable Matchmaking Encryption (DME), an enhanced encryption scheme building upon ME. Utilizing the chameleon hash function, DME offers deniability for both messages and identities, safeguarding user privacy and ensuring the integrity of blockchain-based bidding systems against coercive attempts.

LITERATURE SURVEY

Shamir*et al*

In this paper, we present a groundbreaking cryptographic scheme that facilitates secure communication and signature verification between users without the need for exchanging keys, maintaining key directories, or involving third-party services. The design leverages trusted key

generation centers, issuing personalized smart cards to users upon network entry. These cards empower users to independently sign, encrypt, decrypt, and verify messages, irrespective of the communicating party's identity. Unlike traditional systems, this scheme doesn't require updates to existing cards for new users or coordination among centers. Once all cards are distributed, the centers can cease operations, allowing the network to operate decentralized and indefinitely.

H.Tanaka*et al*

In this paper, we introduce a realization scheme for the modified identity-based cryptosystem initially presented by Shamir at Crypto'84. Our approach capitalizes on the discrete logarithm problem and the computational challenge of factoring large integers comprising two prime numbers. While the system boasts robust security when all participants safeguard their secret keys, it becomes vulnerable if a fixed number of users collaborate to compromise the central secret. To address this susceptibility, we enhance the basic system, elevating its "threshold" through a refined "threshold scheme." Our paper provides comprehensive insights and considerations into this fortified scheme.

O'Neill, C. Peikert, and B. Waters*et al*

In this study, we introduce bi-deniable public-key cryptosystems, enhancing the concept of deniable encryption first proposed by Canetti et al. in 1997. Unlike previous constructions that offered limited deniability, necessitating one party to retain its randomness or employing interactive protocols and external entities, our systems enable both the sender and receiver to equivocate simultaneously. Our approaches are noninteractive, eliminating the need for third-party involvement. One system is rooted in "simulatable encryption," following Damgård and Nielsen's definition, while the other is lattice-based, leveraging the work of Gentry, Peikert, and Vaikuntanathan. These schemes operate within the "multi-distributional" model, enhancing coercion resistance and maintaining essential cryptographic properties.

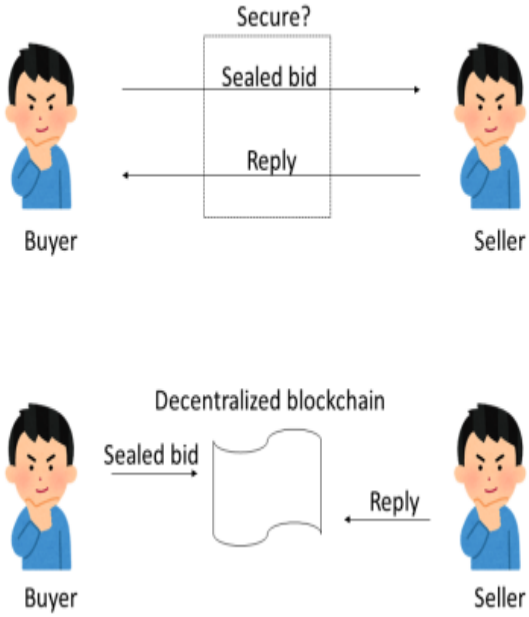
PROBLEM STATEMENT:

Blockchain has inbuilt support for data unchangeable and encryption which is making Blockchain more secure and this advantages forcing application developers to migrate towards Blockchain. Online Bidding is one of the application where bidders will bid for particular tenders and some malicious internal employees will change bidding or tender details to make their favourable person to win bidding and this manipulation will cost huge loss to the bidding system.

PROPOSED METHOD:

Block chain-based bidding systems are becoming increasingly popular nowadays. Due to the properties of Block chain, bidding records are unchangeable. With existing encryption techniques, these bidding records can only be shared by the bidder and the seller. Although this scenario sounds secure, it does not consider a coercion case. A powerful coercer may force the bidding system to open the records stored on the Block chain, and the system loses privacy. To solve this problem, in this paper, in propose paper a new encryption scheme called deniable matchmaking encryption (DME). This new encryption scheme provides deniability not only for the message, but also for the identities. We use the chameleon hash function to make fake message and fake identities indistinguishable from the real message and the real identities. Therefore, the bidding system can use fake information to answer the coercer, and user privacy is kept by the Block chain-based bidding system.

ARCHITECTURE



METHODOLOGY: Blockchain Integration in Bidding Systems

The integration of blockchain technology into bidding systems is a transformative approach to enhancing transparency, security, and efficiency. By leveraging blockchain's decentralized nature and cryptographic hashing capabilities, we can create a bidding environment where transactions are immutable, transparent, and resistant to tampering. This integration not only builds trust among participants but also streamlines the entire bidding process by eliminating intermediaries and reducing administrative overhead.

Deniable Encryption Technique (DME) for Enhanced Privacy

Privacy is paramount in any bidding system. To ensure confidentiality and protect against coercion, we implement the Deniable Encryption Technique (DME). This cryptographic scheme allows only authorized parties, such as sellers and bidders, to decrypt bidding records. By doing so, DME safeguards sensitive information, ensuring that bidding details remain confidential and inaccessible to unauthorized entities.

Chameleon Hash Function for Data Integrity

Maintaining data integrity is crucial in bidding systems. To achieve this, we employ the chameleon hash function, a unique cryptographic tool that generates distinct hash codes for bidding data. This enables easy verification of data integrity, allowing the system to detect any unauthorized modifications or tampering attempts promptly. The chameleon hash function thus serves as a robust layer of security, reinforcing the trustworthiness of the bidding platform.

Bidding Officer Module: Streamlining Tender Creation and Evaluation

A dedicated module for bidding officers is essential for managing tenders effectively. This module enables officers to log in securely, create tenders with initial bidding amounts, and evaluate bids based on predefined criteria, such as the lowest bid amount. Additionally, a winner selection mechanism is implemented to finalize the winning bidder for each tender, ensuring fairness and transparency in the bidding process.

Bidder Module: Empowering Bidders with Seamless Interaction

For bidders, we develop a user-friendly module that facilitates seamless interaction with the bidding platform. Bidders can sign up, log in, and browse available tenders effortlessly. The module also allows bidders to submit their bids, monitor the status of their submissions, and participate in the bidding process transparently and securely, enhancing user engagement and satisfaction.

Extension Concept - Modified DME: Enhancing Accessibility and Security

Building on the DME algorithm, we introduce an extension that enables all participants, including the winning bidder and other bidders, to decrypt

and view winning notifications and bidding details. This modification ensures that transparency is not compromised while maintaining the privacy and security of sensitive information, striking a balance between openness and confidentiality.

User Interface Development: Intuitive and Interactive Design

User experience plays a pivotal role in the adoption and success of any platform. Hence, we focus on designing intuitive, user-friendly interfaces for both bidding officers and bidders. By incorporating intuitive navigation, interactive features, and clear visual cues, we aim to facilitate smooth and efficient interaction, enhancing user satisfaction and platform usability.

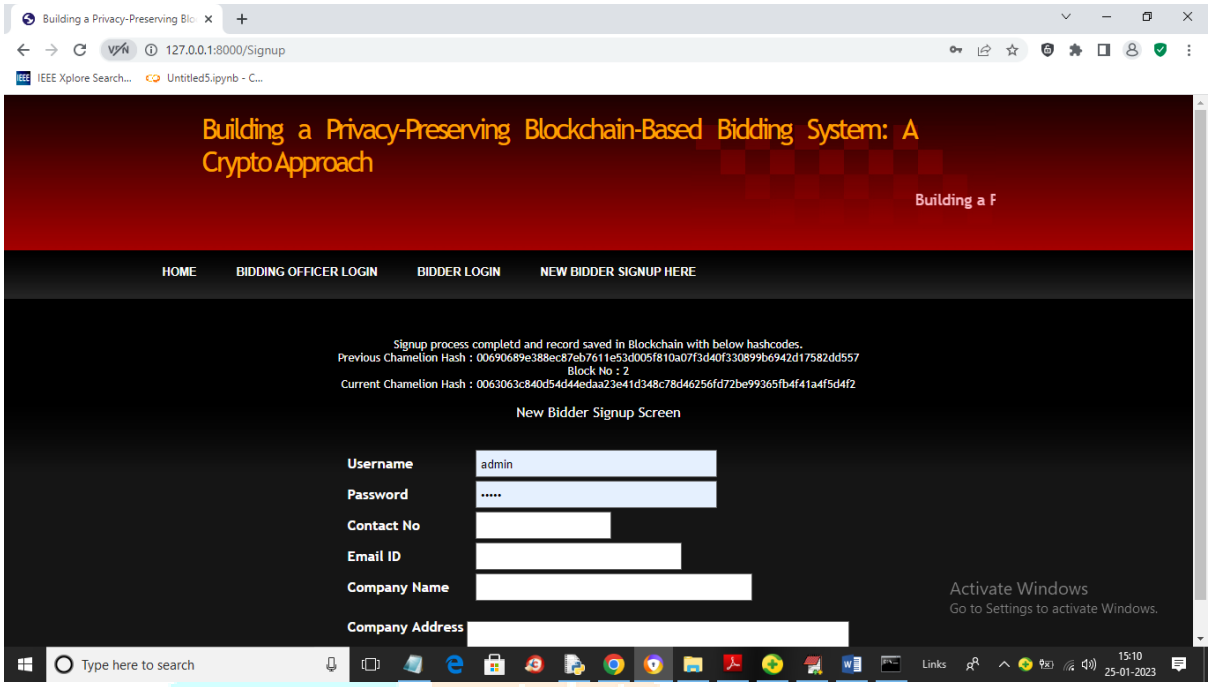
Blockchain Transaction Handling: Ensuring Efficient and Secure Transactions

Efficient handling of blockchain transactions is crucial for the smooth operation of the bidding platform. We develop robust mechanisms to process transactions promptly, ensuring timely confirmation of bidding records. Additionally, error handling and validation procedures are implemented to prevent data inconsistencies, safeguarding the integrity and reliability of blockchain transactions.

Security Measures: Protecting Against Cyber Threats

Cybersecurity is a top priority in our bidding system. We implement a comprehensive set of security measures to protect against potential threats, including unauthorized access, data breaches, and tampering attempts. By employing advanced encryption techniques, multi-factor authentication, and stringent access control mechanisms, we ensure that sensitive bidding information and user credentials are safeguarded against cyber threats, fostering trust and confidence among participants.

RESULTS:



Hash code returned by Blockchain for bidder

CONCLUSION

Implementation of a Privacy-Preserving Blockchain-Based Bidding System using a Crypto Approach addresses the critical need for secure and transparent bidding processes. By leveraging blockchain technology and deniable encryption techniques, the system ensures the integrity and confidentiality of bidding records, safeguarding against manipulation and coercion. The utilization of the Chameleon hash function further enhances data verification and integrity. Additionally, the extension concept allows for broader transparency while maintaining user privacy. The modular design and user-friendly interface facilitate seamless interaction, empowering bidding officers and bidders alike. Overall, this project contributes to enhancing trust, security, and efficiency in online bidding systems.

REFERENCES:

[1] Y.-H. Chen, S.-H. Chen, and I.-C. Lin, ‘‘Blockchain based smart contract for bidding system,’’ in Proc. IEEE Int. Conf. Appl. Syst. Invention (ICASI), Apr. 2018, pp. 208–211.

[2] P. Manimaran and R. Dhanalakshmi, ‘‘Blockchain-based smart contract for E-bidding system,’’ in Proc. 2nd Int. Conf. Intell. Commun. Comput. Techn. (ICCT), Sep. 2019, pp. 55–59. [3] N. Diallo, W. Shi, L. Xu, Z. Gao, L. Chen, Y. Lu, N. Shah, L. Carranco, T.-C. Le, A. B. Surez, and G. Turner, ‘‘EGov-DAO: A better government using blockchain based decentralized autonomous organization,’’ in Proc. Int. Conf. eDemocracyeGovernment (ICEDEG), Apr. 2018, pp. 166–171.

[4] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak, ‘‘A secure publish/subscribe protocol for Internet of Things,’’ in Proc. 14th Int. Conf. Availability, Rel. Secur., New York, NY, USA, 2019, doi: 10.1145/3339252.3340503.

[5] B. Seth, S. Dalal, V. Jaglan, D. Le, S. Mohan, and G. Srivastava, ‘‘Integrating encryption

techniques for secure data storage in the cloud,'' Trans. Emerg. Telecommun. Technol., Sep. 2020, Art. no. e4108, doi: 10.1002/ett.4108.

[6] G. Ateniese, D. Francati, D. Nu nez, and D. Venturi, ''Match me if you can: Matchmaking encryption and its applications,'' in Advances in Cryptology, A. Boldyreva and D. Micciancio, Eds. Cham, Switzerland: Springer, 2019, pp. 701–731.
[7] H. Krawczyk and T. Rabin. (1998). Chameleon Hashing and Signatures. Accessed: Mar. 17, 1998. [Online]. Available: http://eprint.iacr. org/1998/010

[8] A. Shamir, ''Identity-based cryptosystems and signature schemes,'' in Advances in Cryptology, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, pp. 47–53.

[9] Y. Desmedt and J.-J. Quisquater, ''Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?),'' in Advances in Cryptology, A. M. Odlyzko, Ed. Berlin, Germany: Springer, 1987, pp. 111–117.

[10] H. Tanaka, ''A realization scheme for the identity-based cryptosystem,'' in Advances in Cryptology, C. Pomerance, Ed. Berlin, Germany: Springer, 1988, pp. 340–349.

[11] S. Tsujii and T. Itoh, ''An ID-based cryptosystem based on the discrete logarithm problem,'' IEEE J. Sel. Areas Commun., vol. 7, no. 4, pp. 467–473, May 1989.

[12] U. M. Maurer and Y. Yacobi, ''Non-interactive public-key cryptography,'' in Advances in Cryptology, D. W. Davies, Ed. Berlin, Germany: Springer, 1991, pp. 498–507.

[13] D. Boneh and M. Franklin, ''Identity-based encryption from the Weil pairing,'' in Advances in Cryptology, J. Kilian, Ed. Berlin, Germany: Springer, 2001, pp. 213–229.

[14] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Advances in Cryptology, R. Cramer, Ed. Berlin, Germany: Springer, 2005, pp. 457–473.

[15] B. Waters, ''Efficient identity-based encryption without random oracles,'' in Advances in Cryptology, R. Cramer, Ed. Berlin, Germany: Springer, 2005, pp. 114–127.

[16] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, ''Anonymous multireceiveridentitybased encryption,'' IEEE Trans. Comput., vol. 59, no. 9, pp. 1239–1249, Jan. 2010.

[17] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, ''Identity-based encryption with outsourced revocation in cloud computing,'' IEEE Trans. Comput., vol. 64, no. 2, pp. 425–437, Feb. 2015.
[18] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, ''Deniable encryption,'' in Advances in Cryptology, B. S. Kaliski, Ed. Berlin, Germany: Springer, 1997, pp. 90–104.

[19] M. Klonowski, P. Kubiak, and M. Kutyłowski, ''Practical deniable encryption,'' in Theory and Practice of Computer Science, V. Geffert, J. Karhumäki, A. Bertoni, B. Preneel, P. Návrat, and M. Bieliková, Eds. Berlin, Germany: Springer, 2008, pp. 599–609.

[20] A. O'Neill, C. Peikert, and B. Waters, ''Bi-deniable public-key encryption,'' in Advances in Cryptology, P. Rogaway, Ed. Berlin, Germany: Springer, 2011, pp. 525–542.