ISSN NO. 2320-5407

Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/12455
DOI URL: http://dx.doi.org/10.21474/IJAR01/12455

RESEARCH ARTICLE

A COMPARATIVE STUDY OF ZERO KNOWLEDGE PROOF AND HOMOMORPHIC ENCRYPTION IN GUARANTEEING DATA PRIVACY IN BLOCKCHAIN APPLICATIONS

Liz George[1] and Dr. Jubilant J. Kizhakkethottam[2]

1. Asst.Professor, Dept of MCA, St.Joseph's College of Engineering &Technolgy, Kottayam.
2. Professor, Dept.of Computer Science, Saintgits College, Kottayam.

Manuscript Info

Manuscript History
Received: 07 December 2020
Final Accepted: 10 January 2021
Published: February 2021

Key words:-
ZKP, Homomorphic Encryption, Data Privacy, Blockchain

Abstract

Homomorphic Encryption and Zero Knowledge Proofs are two trending concepts that are widely popular as data privacy preservation techniques in a wide variety of applications, especially in those associated with the newly evolved block chain technology which are immutable, distributed and secure. Zero knowledge proof is a cryptographic technique can provide proof that a certain statement is correct, without revealing any details about the statement, while homomorphic encryption allows to perform computations on encrypted data without decrypting it. This article explores the significance of the data privacy aspect provided by both ZKP and Homomorphic Encryption and how it can be effectively used to improvise the privacy of blockchain applications in various domains.

Introduction:-

The concept of blockchain was first introduced in the year 2009 by Satoshi Nakamoto[1]as part of a proposal for digital currency called bitcoin. Since then blockchain technology has been ever evolving, spreading its span to a wide variety of applications, surpassing even the expectations of its creators. The immutable, transparent and distributed features of blockchain provided a solution to 'problem of trust'. It is capable of producing trusted output/transactions between parties who doesn't have mutual trust. The incorporation of cryptographic techniques in blockchain had added to the security of data. Blockchain adopts a peer-to-peer network, where each participant holds a copy of entire transactions/records, bundled together as blocks, making it tamper proof. Each block is linked to its predecessor block by including its cryptographic hash, creating a chain of blocks preserving the integrity. The validity of transactions are ensured by consensus among the participating nodes in the P2P network. From its initial role as a technology to implement the concept of digital currency, blockchain's collaboration with applications in different sectors was triggered by 'smart contracts', which allowed incorporating business logic, specific to applications. Smart contracts are piece of code, with properties of contractual agreement, capable of triggering transactions, when certain conditions are met. As nodes needs to process the data to execute smart contracts various privacy and confidentiality issues may arise. Zero knowledge proof and Homomorphic encryption are two major cryptographic approaches that provides solution to this problem, allowing to share data among devices without compromising security and privacy.

Evolution Of Zero Knowledge Proof:

The concept of Zero knowledge proofs which was accidently discovered in 1980s by MIT researcher Goldwasser et.al[2] while working on problems related to interactive proof systems have come a long way, proving its role in

Corresponding Author:- Liz George
Address:- Asst.Professor, Dept.of MCA, St.Joseph's College of Engineering &Technology, Kottayam.

ensuring the data privacy in many sensitive and significant applications. The growing need of privacy in blockchain applications has fastened the researches in ZKP, resulting in the launch of variations of ZKP from time to time, in view of improving the efficiency. The first among them were Non-Interactive ZKP, a modification of the existing ZKP, removing the inconvenience of successive interaction between the communicating parties [3]. In start of this millennium, range proofs[4] were introduced, which proves that a piece of information lies within a definite range, useful in wide series applications to keep the anonymity of relevant attributes like income or age[5].In the year 2012, zk-SNARK, a better version of NIZK with short proofs and fast verification time was introduced [6].Recently in 2017 Bullet proofs with very short proof size became popular mainly due to the lack of trusted setup, which was a gruelling concern with regard to security for its predecessors. These ZKPs are suitable for implementing range proofs also[7]. By the year 2018 zk-STARK[8] a scalable version of SNARK with no need for trusted setup was introduced, efficient to prevent attack by quantum computers. But this new version had bigger proof sizes when compared to zk-SNARK, making it less compatible for many applications. Latest implementation in the journey of ZKP is supersonic[9], modified version of SNARK with very small proof sizes and faster verification times.

Role of Homomorphic Encryption in privacy:

Homomorphic Encryption had made little progress in the first 30 years after it was first proposed in 1978 [10].HE payed a new way in data privacy management, especially in cloud applications, by allowing computations on encrypted data. 3 variants of homomorphic encryptions were developed in due course of time, namely partially homomorphic encryption, somewhat homomorphic encryption and fully homomorphic encryption. The initial HE schemes proposed belonged to the category of Partial homomorphic encryption which satisfies either the additive or multiplicative property, but not both. A few schemes were fully homomorphic, but with a drawback of increasing size of cipher text with the increase in the no: of operations. [11].The emergence of cloud computing technology and using cloud for mass data storage triggered the need for a mechanism to perform operations on data without compromising data privacy. Craig Gentry [12] in 2009 proposed a way for achieving Fully Homomorphic Encryption, opening new horizons in the application of homomorphic encryption. The major disadvantage of the proposed system was the noise attached with cipher text that increases with each operation. A modified version of Craig's scheme was proposed with smaller cipher text and key by Smart and Vercauteren [13].The scheme that later became most popular was proposed by ZvikaBrakerski et al. [14] which provides better security and performance.

ZKP in Blockchain Applications:

Different types of Zero Knowledge proofs are being used in Blockchain applications depending upon the requirements specified. It has been mainly used in crypto currencies and blockchain applications, to provide proofs about transactional data. The cryptocurrency Zcash [15], uses an extension of Bitcoin Protocol and implements zk-SNARK to provide the proof for the validity of the transaction, without revealing the details regarding transaction like address, amount etc., preventing double spending attacks. Blockchain technology can be effectively collaborated with ZKP to develop anonymous credential systems [16].Using ZKP, the prover can selectively disclose the attributes of the signature issuing authority, maintaining anonymity. Wei Ou et.al [17] proposes a blockchain application with NZKP to perform trustworthy and anonymous transfer of data in vehicle networking .Scalability is an important issue that is faced while using ZKP for blockchain, as algorithms require high computational requirements. Effective schemes that are resistant to quantum attacks is the major research area in ZKP, under current scenario.

Scope Of Homomorphic Encryptions In Blockchain:

The need to preserve data privacy in blockchain applications made Homomorphic Encryption a popular option. Blockchain and IoT are the emerging technologies of last decade. There is an increasing interest for integrating blockchain technology in IoT applications to provide decentralized access. But privacy leakage of data to servers is a major issue in such applications. Implementing Homomorphic Encryption in blockchain based-IoT, provides high security for IoT data in a decentralized mode. [18].Homomorphic encryption can be effectively incorporated to provide transaction authentication in blockchain applications for insurance sector [19].Another important sector which needs utmost data privacy is health care. The statistical analysis of medical records is very critical in research advancements. Homomorphic encryption provides solution to this problem by allowing the statistical analysis on encrypted medical records that are managed by blockchain technology [20].Fully homomorphic encryption is suitable to ensure data privacy, consistent with many existing privacy laws, it has not been progressed yet to satisfy all the expected properties. Large computational overhead, presence of noise and comparatively large size of memory are the drawbacks that have to be rectified.

Conclusion:-

Zero Knowledge proofs and Homomorphic Encryption are two most commonly used cryptographic techniques that can play significant role in ensuring data privacy of applications ranging from Financial, Healthcare to Education. Zero knowledge proofs are more suitable for generating proofs for personal attributes and transactions in applications that needs to preserve the identity of participants. Meanwhile, Homomorphic encryption ensures a different aspect of privacy by allowing computations on encrypted data, making it more suitable for scenarios were analysis of confidential data without compromising privacy is sole priority. A few applications have even tried to incorporate both these techniques. Previously Craig Gentry et.al [21] investigated the possibility of minimizing communication overhead using fully homomorphic hybrid encryption. Both these techniques have been widely implemented in a large range of blockchain applications and its possibilities in more domains are yet to be explored. The feasibility of incorporating both these techniques in a single application to provide identity security as well as data security is a path that has be considered and researched.

References:-

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
2. S. M. W. Oded Goldreich, "Proofs that yield nothing but their validity and a methodology of cryptographic protocol design," in 27th Annual Symposium on Foundations of Computer Science, 1986.
3. F. P. S. Blum M, "Non-interactive zero-knowledge and its applications," in Proceedings of the Annual ACM Symposium on Theory of Computing, 1988.
4. B. F, "Efficient proofs that a committed number lies in an interval," Lecture Notes in Computer Science, vol. 1807, p. 431–444, 2000.
5. T. K. C. V. W. A. K. E Morais, "A survey on zero knowledge range proofs and applications," SN Applied Sciences, 2019.
6. R. C. C. T. Nir Bitansky, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in Proceedings of 3rd innovations in Theoritical Computer Science Conference, 2012.
7. J. B. D. B. P. P. W. G. M. Benedikt Bunz, "Bulletproofs: Short Proofs for Confidential Transactions and More," in Proceedings - IEEE Symposium on Security and Privacy, 2018.
8. B. Y. H. M. R. Eli Ben-Sasson, "Scalable, transparent, and post-quantum secure computational integrity," 2018.
9. B. F. S. Benedikt Bünz, "Transparent SNARKs from DARK Compilers," in International Conference on the Theory and Applications of Cryptographic Techniques , 2020.
10. L. A. M. L. D. Ronald L. Rivest, "On data banks and privacy homomorphisms," in foundations of secure computation, 1978.
11. D. M. Freeman, "Homomorphic Encryption and the BGN Cryptosystem," 2011.
12. C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in Proceedings of the forty-first annual ACM symposium, 2009.
13. F. V. N.P. Smart, "Practice and Theory in Public Key Cryptography," 2010.
14. Z. B. a. C. G. Vaikuntanathan, "Fully Homomorphic Encryption without Bootstrapping," in International
15. Conference on Information Technology Convergence and Services, 2012.
16. C. G. G. Eli Ben-Sasson, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in Proceedings of 2014 IEEE Symposium on Security and Privacy, 2014.
17. L. Jan Camenisch, "'An efficient system for non transferable anonymous credentials with optional
18. anonymity revocation," in Advances in Cryptology—EUROCRYPT, 2001.
19. M. D. a. E. L. Wei Ou, "A Decentralized and Anonymous Data Transaction Scheme Based on Blockchain and Zero-Knowledge Proof in Vehicle Networking," in Collaborative Comput. Netw. Appl. Worksharing, 2019.
20. S. K. Rakesh Shrestha, "Integration of IoT with blockchain and homomorphic encryption: Challenging
21. issues and opportunities," Advances in Computers, vol. 115, pp. 293-331, 2019.
22. L. X. D. T. Xiao, "Insurance Block: A Blockchain Credit Transaction Authentication Scheme Based on
23. Homomorphic Encryption," in International Conference on Blockchain and Trustworthy Systems , 2019.
24. S. S. Mahdi Ghadamyari, "Privacy-Preserving Statistical Analysis of Health Data Using Paillier
25. Homomorphic Encryption and Permissioned Blockchain," in IEEE International Conference on Big Data, 2019.
26. J. G. I. C. P. Craig Gentry, "Using Fully Homomorphic Hybrid Encryption to Minimize Non-interative
27. Zero-Knowledge Proofs," Journal of Cryptology, 2014.