ON THE BLOCKCHAIN BASED CIPHERTEXT POLICY USING ATTRIBUTE BASED ENCRYPTION

[1]Dr.S Hemalatha, [2]Nellore Lakshmi Keerthana ,[3] Nithya Shree J , [4]Swetha k

[1]Professor, Deptarment of Cse, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
[2]Student, Deptarment of Cse, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
[3] Student, Deptarment of Cse, Panimalar Institute of Technology, Chennai, Tamil Nadu, India
[4] Student, Deptarment of Cse, Panimalar Institute of Technology, Chennai, Tamil Nadu, India

---***---

Abstract - *It is human instinct to anticipate occasions later on moreover, plan as necessities are. As requirements are, the chance of permitting future occasions to trigger the unscrambling of a message is such an encryption portion we regard to be essential in the current data age. In this paper, we propose an assortment of Attribute-Based Encryption, called Event-Based Encryption, that will help stay away from severely masterminded assaults. In EBE, we endeavor to unscramble the messages later on after an occasion is affirmed. We depict how EBE can be utilized by introducing a situation where a will is unscrambled when an individual has been admitted dead. To accomplish this, we present a decentralized information sharing association loaded up with blockchain improvement that guarantees information encounters a concentrated checking measure before it is perceived to the affiliation. This attested information is helpful in picking current genuine variables required for the statement of the event of occasions and is too obliging in confining ill-disposed assaults. Our framework uses multi-authority ABE plans, and a decentralized information sharing stage to accomplish our objective. The significant obligation of this evaluation is the empowering of different parties, each with completely insisted prohibitive information, to work together to affirm the event of an occasion. This occasion accreditation should trigger the disentangling of a message. We incorporate the different vocations of our way of thinking similarly, portray the supportive and secure nature of EBE utilizing mathematical outcomes.*

***Key Words*: Decentralized data sharing, blockchain, event-based encryption, adversarial attacks.**

1. INTRODUCTION

A will is a legitimate report that allows a person to convey their cravings of how they should fit their bounty and property at death. The possibility of making a will generally raise various unexpected sentiments like the fear of death, the anxiety of maybe making the contention in the family, and the financial inconveniences caused for the meaning of a will by a lawful advisor. Regardless of the way that we can't encourage the sensations of fear and nerves identified with the conviction of death, or settle the trouble the death of a relative may trigger in a family after, we are prodded to use EBE to take out the arbiter (lawyer) in a situation like this. EBE may help in diminishing the financial load of the individual creating the will. By this, EBE hopes to unscramble a message (will) when an event occurs (passing), without the necessity for an agent.

2. RELATED WORK

2.1 TURING-COMPLETE BLOCKCHAIN SYSTEMS OR SMART-CONTRACTS

A keen arrangement is required to ensure that a comprehension between two social affairs is respected. An outline of such a system is the Ethereum project, which intends to support the satisfaction of veritable trades without the necessity for delegates. Blockchain development ensures the execution of keen arrangements through a decentralized procedure for regarding contracts among qualified get-togethers. The comparable qualities between our philosophy and a canny agreement structure meet in the yearning to abstain from untouchables for consent to be respected.

2.2 ATTRIBUTE BASED ENCRYPTION SCHEMES

Valuable encryption is construction for versatile data sharing that ensures that different recipients of data see different pieces of data. A commendable outline of valuable encryption is ABE, which is identified with access conditions. In ABE, a customer chooses the game plan of qualities that can unravel a message similar to a formula over attributes. For example, a customer can encode a message that ensures that solitary understudies that go to Howard University can unravel it.

2.3 TIME LOCK ENCRYPTION SCHEMES

We likewise draw motivation from prior work done by, where they endeavour to finish a Time-Lapse case. Our work changes in the way that they attempt to interpret a message. Their strategy joins the disentangling of a message after a specific time has passed. Notwithstanding, we unscramble a message subject to the declaration of an occasion. The practically identical characteristics of the two methodologies lay on the way that the two of them depend upon future occasions; in any case, their procedure is exclusively normal.

Then again, we depend upon the event of a future occasion occurring, which isn't, all things considered, a confirmation.

3. LITERATURE SURVEY

TITLE: Enigma: Decentralized Computation Platform with Guaranteed Privacy.
AUTHOR: Howard Shrobe; David L. Shrier; Alex Pentland;
YEAR: 2018.
DESCRIPTION:

A conveyed association enables different get-togethers to together store and run estimations on data while keeping the data completely covered up. Puzzle's computational model relies upon a significantly upgraded variation of secure multi-party estimation, guaranteed by a specific secret sharing arrangement. For limit, we use a changed appropriated hash-table for holding secret-shared data. An outside blockchain is utilized as the controller of the association, which regulates access control and characters and fills in like a fixed log of events. Security stores and costs support the movement, rightness, and sensibility of the circumstance. Like Bitcoin, Enigma dispenses with the prerequisite for a trusted in untouchable, engaging independent control of individual data. Strangely, customers can grant their data to cryptographic confirmations concerning their insurance.

TITLE: Towards Federated Learning Approach to Determine Data Relevance in Big Data.
AUTHOR: Ronald Doku; Danda B. Rawat; Chunmei Liu;
YEAR: 2019
DESCRIPTION:

In recent years, information has expanded to gaudy degrees; along these lines, gigantic information has gotten the main role behind the improvement of various AI types of progress. Regardless, the relentless season of information in the data age tends to a needle in the bundle issue, where it has gotten testing to pick significant information from a stack of unimportant ones. This has accomplished quality over whole issues in information science where a great deal of information is being conveyed, regardless, by a wide margin, its greater part is irrelevant. Likewise, a gigantic piece of the data and the resources expected to reasonably plan AI models are guaranteed by essential tech affiliations, achieving a centralization issue. Consequently, consolidated learning attempts to change how AI models are set up by accepting a passed-on AI approach. Another promising development is the blockchain, whose lasting nature ensures data decency. By joining the blockchain's trust framework and consolidated learning's ability to disturb data centralization, we propose a system that chooses appropriate data and stores the data in a decentralized manner.

TITLE: Proof-of-Property - A Lightweight and Scalable Blockchain Protocol.
AUTHOR: Christopher Ehmke; Florian Wessling; Christoph M. Friedrich;
YEAR: 2018

The improvement of blockchain propels from financial applications to various fields raises the issue of an extending size of data set aside in the blockchain. Tragically, new individuals from the blockchain network are expected to download the whole blockchain to gain a layout of the state of the structure and to affirm moving toward trades. Approaches like IOTA, Seg Wit, or the Lightning Network endeavor to settle the flexibility issues of blockchain applications. Incredibly, they base on methods thwarting the blockchain's improvement rather than reducing the issues arising out of a creating chain or familiarize groundbreaking thoughts with ousting the straight blockchain all around. The procedure proposed in this paper relies upon the chance of Ethereum to keep the state of the structure unequivocally in the current square anyway further seeks after this by including the significant piece of the current system state in new trades as well. This enables various individuals to affirm moving toward trades without downloading the whole blockchain from the outset. Following this idea use cases can be maintained that require versatile blockchain development yet not actually an unsure and complete trade history.

TITLE: A Secure and Practical Blockchain Scheme for IoT.
AUTHOR: Hongyang Liu; Feng Shen; Zhiqiang Liu;
YEAR: 2019.
DESCRIPTION:

With features such as decentralization, consistency, tamper resistance, non-repudiation, and pseudonym, blockchain technology has the potential to strengthen the Internet of Things (IoT) significantly, thus opening an intriguing research area in the integration of blockchain and IoT. However, most existing blockchain schemes were not dedicated to the IoT ecosystem and hence could not meet the specific requirements of IoT. The designs above allow for supporting faulty-shards-tolerance and asynchronous network model, which could not be sustained in Chainspace, and keeping high efficiency as well. Last but not least, VChain also inherits the merits of Chainspace to separate the execution and verification of smart contracts for privacy.

4. EXSISTING SYSTEM

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key).

5. PROPOSED SYSTEM

In EBE, we endeavor to unscramble the messages later on after an occasion is affirmed. We represent how EBE can be utilized by introducing a situation where a will is unscrambled when an individual has been affirmed dead.

6. MODULES

6.1 USER INTERFACE DESIGN
6.2 FILE UPLOAD
6.3 DOUBLE ENCRYPTION PROCESS
6.4 REQUEST TO ADMIN
6.5 RESPONSE FROM ADMIN
6.6 DOWNLOAD THE FILE
6.7 HACKER REQUEST

DESCRIPTION

6.1 USER INTERFACE DESIGN

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password, we can't enter into login window to user window it will shows error message. So, we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So, server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

6.2 FILE UPLOAD

In this module, after login the owner will upload the file details and it will be stored in the database.

6.3 DOUBLE ENCRYPTION PROCESS

In this module, when the file is getting uploaded in the back-end there happens the double encryption process and it will be stored in the database.

6.4 REQUEST TO ADMIN

In this module, the user will be sending the file request to the admin for which files, the user needs the access. Without the permission form the admin, the user can't able to download the file.

6.5 RESPONSE FROM ADMIN

In this module, the admin will be giving the acceptance to the user for which file needs the access. After the acceptance, the file key will be sent to the user.

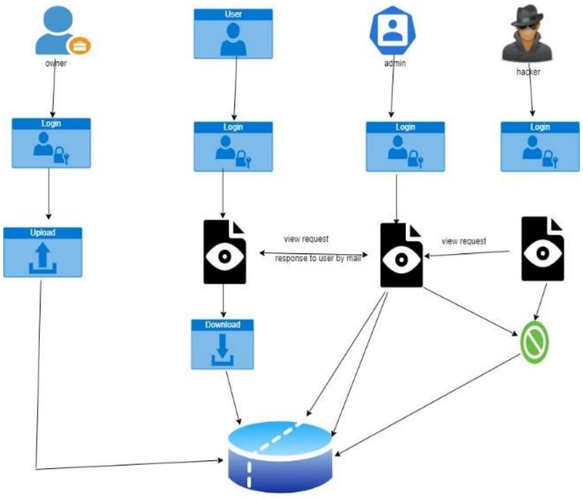
6.6 DOWNLOAD THE FILE

In this module, after getting the key from the admin, the user can download the file using the key provided by the admin.

6.7 HACKER REQUEST

In this module, hacker request a file after received by admin and view. After Admin has been blocked.

7. SYSTEM ARCHITECTURE



8. FUTURE ENHANCEMENT

Functional encryption is still in its infancy and many fascinating open problems remain. We conclude with several directions for future work.

9. CONCLUSIONS

In this work, we presented a variant of ABE, called EBE that aims to decrypt messages in the future when the occurrence of an event is confirmed. We illustrate how EBE can be employed by presenting a scenario where a will is decrypted when an individual has been confirmed dead. We discuss the decentralized data sharing approach on which EBE is implemented on. This decentralized data-sharing network is powered by the blockchain technology which ensures data undergoes a thorough vetting process before it is accepted to the network to avoid adversarial attacks. Specifically, we used the vetted data as a knowledge base in our work to confirm the occurrence of an event. We incorporated various NLP techniques and modified an existing ABE scheme to design this variant of ABE we call EBE.

REFERENCES

[1] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, no. 2014, pp. 1–32, 2014.

[2] D. Boneh, A. Sahai, and B. Waters, “Functional encryption: Definitions and challenges,” in Theory of Cryptography Conference, pp. 253–273, Springer, 2011.

[3] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 457– 473, Springer, 2005.

[4] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertextpolicy attribute-based encryption,” in 2007 IEEE symposium on security and privacy (SP’07), pp. 321–334, IEEE, 2007.

[5] M. O. Rabin and C. Thorpe, “Time-lapse cryptography,” 2006.

[6] I. F. Blake and A. C.-F. Chan, “Scalable, server-passive, user-anonymous timed release public key encryption from bilinear pairing.,” IACR Cryptology ePrint Archive, vol. 2004, p. 211, 2004.

[7] R. L. Rivest, A. Shamir, and D. A. Wagner, “Time-lock puzzles and timed-release crypto,” 1996.

[8] G. Zyskind, O. Nathan, and A. Pentland, “Enigma: Decentralized computation platform with guaranteed privacy,” arXiv preprint arXiv:1506.03471, 2015.

[9] J. Ge, J. Ning, and A. Yu, “Cybervein: A dataflow blockchain platform,” 2018.

[10] OpenMined, “Openmined: Building safer artificial intelligence.,” 2018.

[11] R. Craib, R. Bradway, X. Dunn, and J. Krug, “Numeraire : A cryptographic token for coordinating machine intelligence and preventing overfitting,” 2017.

[12] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in International Conference on Machine Learning, pp. 201–210, 2016.

[13] H. Turesson, A. Roatis, H. Kim, and M. Laskowski, “Deep learning models as proof-of-useful work: A smarter, utilitarian scheme for achieving consensus on a blockchain,” 2018.

[14] R. Doku, D. B. Rawat, and C. Liu, “Towards federated learning approach to determine data relevance in big data,” in 2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI), pp. 184–192, 2019.

[15] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system. bitcoin,” 2009.