**Building a Privacy-Preserving Blockchain-Based Bidding System: A Crypto Approach**

|  |  |
| --- | --- |
| **Mohana Krishnan. R**  Department of CSE  Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala  Engineering College,Avadi.  [Rmohanakrishnan02@gmail.com](mailto:%20Rmohanakrishnan02@gmail.com) | **Nikhil. B**  Department of CSE  Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala  Engineering College,Avadi.  [Vishalnikhil0307@gmail.com](mailto:%20Vishalnikhil0307@gmail.com) |
| **Kanagasabai. K**  Department of CSE  Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala  Engineering College,Ava[di](mailto:nivedilip2072@gmail.com)  [Kanagasabai20@gmail.com](mailto:%20Kanagasabai20@gmail.com) | **Sunil Ahamed. S**  Department of CSE  Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala  Engineering College,Avadi.  [suniliplay@gmail.com](mailto:%20suniliplay@gmail.com) |
| **Victor Jose.M(CSE)**  Department of CSE  Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala  Engineering College,Avadi.  [mvictorjose@veltechmultitech.org](mailto:mvictorjose@veltechmultitech.org) |  |

**Abstract- Blockchain-primarily based totally bidding structures have become more and more more famous nowadays. Due to the homes of blockchain, bidding facts are unchangeable. With present encryption techniques, those bidding facts can best be shared via way of means of the bidder and the seller. Although this situation sounds secure, it does now no longer recollect a coercion case. A effective coercer might also additionally pressure the bidding gadget to open the facts saved at the blockchain, and the gadget loses privateness. To resolve this problem, on this paper, we introduce a brand new encryption scheme known as deniable matchmaking encryption (DME). This new encryption scheme offers deniability now no longer best for the message, however additionally for the identities. We use the chameleon hash feature to make faux message and faux identities indistinguishable from the actual message and the actual identities. Therefore, the bidding gadget can use faux records to reply the coercer, and consumer privateness is stored via way of means of the blockchain-primarily based totally bidding gadget.**

***KEYWORDS: Deniable encryption, matchmaking encryption, chameleon hash function, blockchain-based bidding system.***

1. **INTRODUCTION**

Recently, blockchain has become highly popular, especially in commerce, and it has influenced the growth and usefulness of many commercial applications. With the decentralized and hash-chained nature of blockchain, commercial applications can eliminate the problem of whether a third-party or com- munication channel is trustworthy, which is the most critical problem for a bidding system. The difference between traditional and blockchain-based bidding systems is shown in Figure 1. In traditional bidding systems, a buyer seals his or her bid to protect the information and sends it to a seller during the auction. The buyer must ensure that the sealed bid is securely delivered to the seller, without any distortion or information leakage. In a blockchain-based bidding system, the buyer can confirm that his or her bid is safely delivered to the seller and cannot be changed by any adversaries. As a result, the market share of blockchain-based bidding systems is increased.

In a bidding system, the most important property is the privacy of the identities of the transaction both sides and the bidding content. This is not the case in which the communication peers are required to be authenticated, such as the IoT (Internet of Things) scenario or the normal cloud storage case. Instead, for a fair competition for the price of the auction, no buyer should obtain any information about other buyers’ prices or identities; only the seller and the buyer who sealed the bid can decrypt the bid successfully, and the sealed bid should not leak any identifying information to others. If the buyer’s identity or their bid information leaks to other competitors, the auction becomes unfair and untrustworthy. Thus, an encryption system that can be operated without explicit identities is required. In 2019, Ateniese *et al.* pro- posed an encryption scheme called matchmaking encryption (ME) , which can hide senders’ and receivers’ identities simultaneously. In an ME scheme, the sender and receiver identities are hashed and used in the encryption process. No outsider can obtain identity information, including the sender or the receiver, from a ciphertext. Only a party who knows the sender and the receiver of a ciphertext can cor- rectly decrypt the ciphertext with the receiver’s secret key. Therefore, ME is a good candidate that completely fits into the blockchain-based bidding system.

Although ME fits blockchain-based bidding systems, there are still some ‘‘out-of-rules’’ problems that can break the security and privacy of applications. For example, in some countries, the government may try to trace an opposing party’s messages with the excuse of circumventing fake news. The government may force some service providers to hand over specified users’ secrets. The bidding system is also a case that faces problems. If there is a coercer who forces the buyer, seller or key publisher to reveal their private secrets, the ME system crashes, and the bidding system becomes unsafe. Therefore, we need other tools to enhance the ME system.

To address the problem of coercing users into revealing their information, we introduce the idea of deniable encryp- tion. Deniable encryption is now widely used when a user wants to prevent a message from being coerced. To deal with a malicious coercer, the deniable encryption technique can make the user convince the coercer with a fake message and keep the true message secret. This is a better way to protect user privacy than simply denying coercion requests.

Regarding ME, not only the message, but also the iden- tities should be deniable. That is, given an ME ciphertext, we want to make the coercer believe the fake message, the fake sender and the fake receiver, so that the real sender, the real receiver and the real message are protected. For this reason, in this paper, we propose an encryption scheme called deniable matchmaking encryption (DME). The scheme is enhanced from identity-based matchmaking encryption (IB-ME), which was proposed by Giuseppe Ateniese *et al.* in 2019 [6]. The concept is shown in Figure [2](#_bookmark2). We use the chameleon hash function as a verification tool in the decryption phase. The chameleon hash is a cryptographic hash function which can easily find a collision with a secret trapdoor. The trapdoor collision property of chameleon hash makes it possible to forge a fake message that has the same hash value as the real message; therefore, both the true mes- sage and the fake message can pass the verification check in the decryption phase. When encryption is performed, the true message is protected with the true sender and the true receiver by IB-ME, while the fake message is protected by the fake entities. When being coerced, the fake message and the fake identities are provided to the coercer. Therefore, the real message and the real identities are kept secret.

# **Literature Survey**

**Audio Watermarking for Security and Non-Security Applications[1]:** Maha Charfeddine , Eya Mezghani , Salma Masmoudi , Chokri Ben Amar and Hesham Alhumyani published in 2022. Description :The digitization of audiovisual data is significantly increasing. Thus, to guarantee the protection of the intellectual properties of this digital content, watermarking has appeared as a solution. Watermarking can be used in reality in several types of applications that target two different contexts: the first for security applications and the second for non-security ones. In this paper, we carry a big interest in studying these two types of applications. Moreover, we propose a first digital watermarking scheme for security copyright protection applications, where we have involved neural network architecture in the insertion and detection processes, and integrated some masking phenomena of the human psychoacoustic model with linear predictive coding spectral envelope estimation of the audio file.

**HEVC Watermarking Techniques for Authentication and Copyright Applications: Challenges and Opportunities [2]:**

Ali A. Elrowayati , Mohamed A. Alrshah , Mohammad Faiz Liew Abdullah and Rohaya Latip, published in 2020. Recently, High-Efficiency Video Coding (HEVC/H.265) has been selected to update preceding video coding standards, consisting of H.263 and H.264. Despite the performance of HEVC, it nonetheless lacks dependable and realistic functionalities to assist authentication and copyright applications. In order to offer this assist, numerous watermarking strategies had been proposed through many researchers all through the previous couple of years. However, the ones strategies are nonetheless affected by many problems that want to be taken into consideration for destiny designs. In this paper, a Systematic Literature Review (SLR) is delivered to perceive HEVC demanding situations and ability studies instructions for fascinated researchers and developers. The time scope of this SLR covers all studies articles posted over the last six years beginning from January 2014 as much as the give up of April 2020. Forty- articles have met the standards of choice out of 343 articles posted on this region all through the referred to time scope. Anew class has been drawn observed through an identity of the demanding situations of imposing HEVC watermarking strategies primarily based totally at the evaluation and dialogue of these selected articles. Eventually, guidelines for HEVC watermarking strategies had been indexed to assist researchers to enhance the prevailing strategies or to layout new green ones.

**A Blockchain Ethereum Technology-Enabled Digital Content: Development of Trading and Sharing Economy Data [3]:**

Umair Khan , Zhang Yong An and Azhar Imran, published in 2020. The concept of a shared financial system turns into one of the agencies as an corporation type. Especially with the superior improvement of virtual clever gadgets and the internet, numerous sorts of the mutual financial system had been superior in accord with the want for sharing of separate income. Shareable commodity and virtual content material also are searching for to utilize. When virtual content material is used as a sharing financial system, diverse viable threats may also rise up withinside the route of transactions, the ability for theft, alteration, and hacking of contents. This paper gives a complete review of the safety and privateness of Blockchain. Blockchain promise obvious, tamper-evidence and stable structures which could permit novel solutions, particularly whilst mixed with clever contracts. In this research, we proposed a content material safety and transaction technique the use of Blockchain Ethereum Technology. The encryption set of rules is included in proposed machine to make obvious transactions and it's also applied on content material itself to save you from clever forgery and hacking. The experimental effects characterize that the proposed technique has sturdy ability to decorate transactions transparency via way of means of minimizing the safety threats in virtual content material transactions.

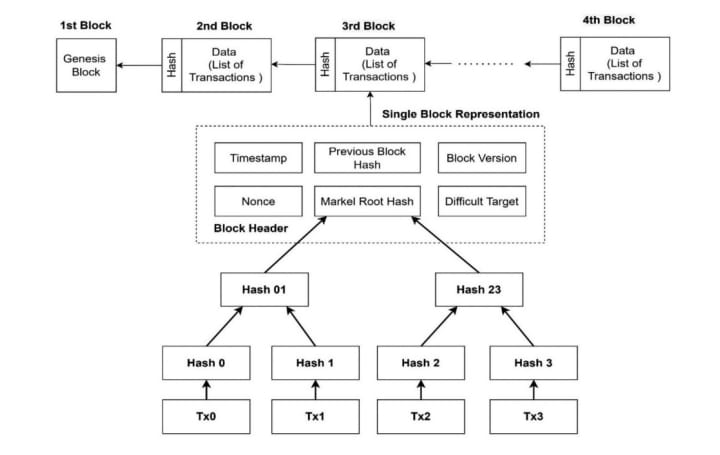
**Rate-Distortion-Preserving Forensic Watermarking Using Quantization Parameter Variation [4]:**

Hannes Mareen , Martijn Courteaux , Johan De Praeter , Md. Asikuzzaman , Glenn Van Wallendael and Peter Lambert, published in 2020. Watermarking enables the identification of digital pirates that illegally redistribute copyright protected videos. One of the main challenges is for the watermark to be imperceptible, while not increasing the video bit rate. Additionally, the system should be robust to attacks that attempt to remove the watermark. Therefore, this paper proposes a robust watermarking technique that does not degrade the video quality nor negatively affect the video bit rate. In other words, it preserves the video encoders compression efficiency or rate-distortion performance. For watermark embedding, the quantization parameters are varied during video compression. As a result, different compression artifacts are introduced, although they do not distort the video more than those that occur during ordinary video compression. The collection of artifacts represents the watermark and is used for watermark detection. The experimental results prove that the proposed approach retains the rate-distortion performance better than state-of-the-art techniques. Furthermore, the watermarks are robust to recompression and noise attacks. In conclusion, the proposed method enables content providers to perform forensic watermarking without affecting the compression efficiency.

# **III. Proposed System Methodology**

**PROPOSED SYSTEM ARCHITECTURE**

All users must register before using the system; The authenticator is responsible for verifying the legitimacy of requests sent by requestors to the data owners system. On a shared server, a security management model designed for password-authenticated users allows access to shared files. Although the scheme simplifies security management efforts, all backups and sharing files are still reside on the sharing server. Also, the file sharing policy relies on the authentication mechanism on the sharing server and is based on the users password to extract the key. Data sharing is one of important applications in computing, especially for enterprise. Usually, an enterprise may authorize some entities to share its remote data under the its defined policy. Data owner is an entity whose massive data will be uploaded to the servers for storage and processing. The data owner registers the copyright of the digital works on the system. During the registration process, the data information of the digital works needs to be extracted and stored; The data owner uploads these data blocks along with their corresponding signatures to the server. The data stored in the server is often shared across multiple users in many storage applications. In such a scheme, the sensitive information can be protected and the other information can be published. It makes the file stored in the server able to be shared and used by others on the condition that the sensitive information is protected, while the remote data integrity is still able to be efficiently executed.



**Fig. 1. Technical Architecture**

Anyone needs to verify the Digital Information Ownership information, the proposed system is used to trace the entire process of circulation to investigate and retrieve the information. Hence, the system provides the query functions. The data query layer consists of sets of querying structures that access, process, forward or respond to queries posed on the system. Queries on the systems may be requests to access data from the existing database infrastructure. The data query layer directly interfaces with the data structuring and provenance layer and has mechanisms, implemented to interpret and translate actions between the data structuring and provenance layer and the outside environment.

**I. HARDWARE REQUIREMENT**

* Operating System
* Processor
* Memory

## **A. Operating System**

A running device (OS) is device software program application that manages pc hardware, software program application resources, and presents. Time-sharing running structures timetable duties for green use of the device and might also consist of accounting software program for value allocation of processor time, mass storage, printing, and different resources. Hardware features together with enter and output and reminiscence allocation, the working machine acts as a middleman among applications and the laptop hardware, despite the fact that the utility code is normally achieved at once via way of means of the hardware and often makes device calls to an OS feature or is interrupted via way of means of it. Operating structures are discovered on many gadgets that incorporate a computer from cells telephones and online game consoles to net servers and supercomputers.

***B. Processor***

A processor plays arithmetical, logical, input/output (I/O) and different simple commands which are handed from a running system (OS). Most different methods are depending on the operations of a processor. The phrases processor, valuable processing unit (CPU) and microprocessor are usually related as synonyms. Most humans use the word “processor” interchangeably with the term “CPU” nowadays, it's miles technically now no longer accurate because the CPU is simply one of the processors interiors a non-public computer (PC). The Graphics Processing Unit (GPU) is any other processor, or even a few tough drives are technically able to do some processing.

**C. Memory**

Memory is the digital maintaining location for the commands and information a pc wishes to attain quickly. It's in which data is saved for fast use. Memory is one of the fundamental capabilities of a laptop. Memory is likewise utilized by a computer's working system, hardware and software.

# **II. software requirements**

* Python
* Python RESTful
* SQL Server
* Frontend Technologies
* HTML, CSS, JavaScript
* Angular

## **A. Python**

Python is a runtime environment object oriented high-level computer program with dynamic semantics. Since there is no compilation phase, the modify cycle is extremely fast. A source level breakpoint allows users to inspect local and global variables, run arbitrary expressions, set breakpoints, step via the code one line at a time, and so on. Python provides modules and packages, which assists with programming modularity and code reuse.

***B. Python RESTful***

Rest (Representational State Transfer) API Python framework is a fixed of utilities primarily based totally on werkzeug to effortlessly construct Restful API. It is simple to configure and extends with ease. It does now no longer determine how the statistics may be rendered, nor every other decision. Instead, it’s an effortlessly extensible structure to construct one’s API. Python REST API Framework has now no longer been created for the standard case however hooks on to important aid companies with unique view management, and unique manner of showing statistics.

***C*. *SQL Server***

Microsoft SQL Server is a relational database control gadget evolved with the aid of using Microsoft. As a database server, it's far a software program product with the number one feature of storing and retrieving information as asked with the aid of using different software program programs—which might also additionally run both at the equal laptop or on any other laptop throughout a network (along with the Internet). Microsoft markets as a minimum a dozen unique variants of Microsoft SQL Server, aimed toward unique audiences and for workloads starting from small single-gadget programs to massive Internet-going through programs with many concurrent users.

***D. Frontend Technologies***

Front-give up technology are a fixed of technology used to increase the consumer interface of net pages and applications. With front-give up technology, builders create the whole lot from layout and shape to animation we see on display screen whilst beginning a website, net utility, or cell app. These technology play a important function in enticing the customers and inspiring and riding them in the direction of the preferred action. An utility’s seamless front-give up generation makes the utility smooth to apply and recommendable to others. Therefore, companies striving to decorate consumer interaction, interactivity, performance, and the general appearance in their utility ought to understand the significance of front-give up technology. The number one intention of front-give up improvement strategies and gear is to allow cell and net builders to enhance their performance and enjoy a quicker, extra straightforward, and higher improvement process.

***E. HTML, CSS, JavaScript***

The HyperText Markup Language or HTML is the usual markup language for files designed to be displayed in an internet browser. It is regularly assisted via way of means of technology along with Cascading Style Sheets (CSS) and scripting languages along with JavaScript. HTML can embed packages written in a scripting language along with JavaScript, which impacts the conduct and content material of net pages. The inclusion of CSS defines the appearance and format of content material. The World Wide Web Consortium (W3C), former maintainer of the HTML and present day maintainer of the CSS standards, has advocated the usage of CSS over express presentational HTML considering the fact that 1997. A shape of HTML, referred to as HTML5, is used to show video and audio, basically the usage of the element, collectively with JavaScript. JavaScript (js) is a lightweight object-orientated programming language that's utilized by numerous web sites for scripting the webpages. It is an interpreted, full-fledged programming language that allows dynamic interactivity on web sites whilst implemented to an HTML document. It become added withinside the yr 1995 for including packages to the webpages withinside the Netscape Navigator browser. Since then, it's been followed via way of means of all different graphical net browsers. With JavaScript, customers can construct contemporary-day net programs to have interaction immediately with out reloading the web page each time. The conventional internet site makes use of js to offer numerous kinds of interactivity and simplicity.

***F. Angular***

Angular is a platform and framework for constructing single-web page purchaser programs the usage of HTML and TypeScript. Angular is written in TypeScript. It implements middle and optionally available capability as a fixed of TypeScript libraries which you import into your programs.

# **IV. Result and analysis**

For the computational cost, denote *et* , *h*, *ch* and *e* as the exponential computation, hash function computation, chameleon hash function compu- tation, and bilinear mapping computation, respectively. Our DME focuses on the encryption scheme, so the computation times in **Setup**, **SKGen**, and **RKGen** are equal to that in ME. In the **Enc** and **DeniEnc** algorithms, because our DME generates a fake ciphertext, which has the same hash value as the true ciphertext, the computation time is twice the time of the ME scheme. These algorithms have an additiona computation time for forging the random string, which is used in the chameleon hash function. Finally, in the **Dec** algorithm, the worst decryption case of DME is that the receiver picks the fake ciphertext to decrypt, so the worst computational cost is also twice the computational cost of ME. By doubling the computational cost of ME, we can make a DME scheme, and we think the additional computational cost is justified.

**V. Conclusion**

In this paper, we proposed a new encryption called DME to solve the coercion problem on blockchain-based bidding systems. Using DME on blockchain-based bidding systems, we can preserve the privacy of the buyer and seller identities during the auction. We use a fake buyer and seller pair to cover the real transaction, including the identities and the content. We show that our scheme costs approximately twice the base scheme in both space and computational time for the deniability feature. We believe it is worth the cost to protect the privacy of transaction identities.

**VI. Future Enhancements:**

Our future work will include two directions. First, we will practically implement the whole bidding system on the blockchain. Theoretically, the performance of our scheme is similar to our base scheme, and we still want to know if it is appropriate for real transaction marketing. Moreover, we will consider more attack scenarios against the blockchain system and determine whether there are vulnerabilities other than the cryptographic issue. Second, we want to extend our work to support attribute-based ME. Compared to IB-ME, the attribute-based ME technique will provide more flexibility. The concept was proposed by Ateniese *et al.* and was constructed by Xu*et al.*, but there is still no practical approach developed. The most important challenge is how to hide the attributes, not only their contents but also their labels. We want to cover the sender group with a totally different group. Currently, there is no ABE system that can fully hide identity attributes. However, this will be a major issue in the matchmaking system since without knowing the identity’s attributes, it is impossible to perform successful decryptions. Therefore, we want to take this challenge as our next step. We believe that it will make our deniable matchmaking encryption scheme more useful.

**VII. References:**

[1]"Do not ask me what I am looking for: Index deniable encryption" by P.-W. Chi and Y.-L. Chang, Published in IEEE in 2021.

[2]"Match in my way: Fine-grained bilateral access control for secure cloud-fog computing" by S. Xu, J. Ning, Y. Li, Y. Zhang, G. Xu, X. Huang, and R. Deng, Published in IEEE in 2020.

[3]"CL-ME: Efficient certifi- cateless matchmaking encryption for Internet of Things" by B. Chen, T. Xiang, M. Ma, D. He, and X. Liao, Published in IEEE in 2021.

[4]"Blockchain-based smart contract for E-bidding system" by P. Manimaran and R. Dhanalakshmi, Published in IEEE in 2019.