Pegem Journal of Education and Instruction, Vol. 13, No. 4 , 2023 (pp. 709-728)

RESEARCH ARTICLE WWW.PEGEGOG.NET

AN ENCRYPTION AND REVOCATION SCHEME FOR PERSONAL PRIVACY DATA PROTECTION FOR HIGH-DIMENSIONAL ATTRIBUTE DOMAINS

G.Sirisha[1], ,K. Pooja Chowdary[2], Kolipaka Lahari, [3] K. Vaishnavi, [4]

[1] Assistant Professor, Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

swecsirishaganga@gmail.com,

[2, 3, 4] Department of Information Technology, Sridevi Women's Engineering College, Hyderabad

ABSTRACT: Protecting sensitive information is more important than ever before due to the prevalence of data breaches involving personal information. Stable fact storage and sharing is made possible by integrating Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with blockchain technology. Existing techniques encounter problems such as degraded safety, significant computational complexity, and steeply priced attribute revocation in high-dimensional characteristic domains. In order to tackle such difficult circumstances, this study suggests a new plan. It integrates HAD-FME with SM-ARM for improved security and lower computing costs, uses smart contracts for green revocation, and is part of a three-part system that includes Fast High-dimensional Attribute Domain-based Message Encryption (HAD-FME), an Attribute Revocation Mechanism Based on Sentry Mode (SM-ARM), and a Blockchain-based Model for Personal Privacy Data Protection (BC-PPDP). Following the DLIN assumption and with the pride of forward and backward safety for attribute revocation, security analysis indicates that HAD-FME is effective. Smart contracts and blockchain have shown to be useful in ensuring the safety and privacy of information, and experiments demonstrate that HAD-FME has enhanced computing performance and that SM-ARM has decreased revocation costs compared to current approaches. Data storage and dissemination, attribute invalidation, attribute-centric encryption, blockchain technology, and confidential information are some of the keywords.

KEYWORDS: Prevalence of data, Data breach, Ciphertext, Attribute-Based Encryption, Blockchain, Smart contracts, Data Protection

1. INTRODUCTION

Cloud computing and the IoT are two examples of rapidly developing technologies that have led to the worldwide dissemination of large volumes of personally identifiable information. Businesses are always collecting and analyzing these personal details, using them to create personalized products and services and making a killing. This is fantastic news for consumers and businesses alike, as it means more money in the data tech market. Unfortunately, there

How to cite this article: G.Sirisha1, ,K. Pooja Chowdary2, Kolipaka Lahari, 3 K. Vaishnavi, 4. AN ENCRYPTION AND REVOCATION SCHEME FOR PERSONAL PRIVACY DATA PROTECTION FOR HIGH-DIMENSIONAL ATTRIBUTE DOMAINS.Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 709-728

Source of support: Nil **Conflicts of Interest:** None.

DOI: 10.47750/pegegog.13.04.80

Received: 12.10.2023

Accepted: 22.11.2023 **Published:** 24.12.2023

has been a dramatic increase in the number of incidents of non-public data breaches in recent years due to the lack of robust data safety measures used by enterprises. One example is the practice of keeping information in plaintext on centralized servers.Presently, blockchain and CP-ABE are the centers of attention when it comes to statistical safety measures. As part of the research, it presents several data security approaches, such as verifiable ledger databases

and CP-ABE-based feature revocation. Part A. Data security measures The increasing collection and use of consumer privacy data by agencies has led to the emergence of several privacy facts security methods in industries like as healthcare and clinical research. Green CP-ABE techniques for cloud storage are provided by Chen et al., while blockchain privacy and secrecy security is addressed by Lee et al. Using smart contracts for access control, Wang et al. presented the RCP-ABE personal privacy data protection device. Also, a signature system based on forward-steady attributes that may be traced was presented by Kang et al. Despite the encouraging results, problems such as the high processing cost associated with domain names with several dimensions of attributes continue. B. Revocation of attributes using CP-ABE Attribute revocation has been the subject of several CP-ABE investigations. By combining fast revocation with multi-authority attribute-based encryption, Qian et al. presented a method for private health records that preserve patients' privacy. To make sure that information access permissions are renewed depending on attribute revocation, Chen et al. created a cloud storage device that is consistent with this requirement. Regardless of these improvements, methods such as the ones suggested by Li et al. and Li et al. still need computational value discount, especially in the case of attribute revocation involving IoT devices. Section C: Guaranteed ledger databases There are two main types of ledger databases: DLTs that rely on permission blockchains and CLTs that rely on cryptographic ledgers. The possibility for DLT to provide an unchangeable and verifiable ledger was emphasized by Gorbunova et al. Your Customer (KYC) process plays a vital role for all banks in authenticating the identity of their customers. KYC verification is crucial to prevent banks from being used by illegal elements for money laundering activities such as drug trafficking, terrorism and other crimes. Manual KYC process in mainstream at present is less secure, time consuming and outdated. Since Blockchain offers features like decentralization, immutability and security, these limitations can be eliminated by using Blockchain based KYC verification. In this paper, we have proposed decentralized KYC verification process using Ethereum Blockchain platform. It would allow all the banks in the Blockchain network to verify and vote for legitimacy of the data provided by the customer. Depending on number

of votes KYC status of customer gets stored on the Blockchain. Major enhancement in our proposed method is, banks can also vote for other banks if any bank is tampering with the KYC data and it will get removed from the network based on this voting. In this way, Blockchain can be used to improve the efficiency of KYC process with its distinctive features. Know Your Customer (KYC) is a standard in the finance industry which ensures banks/financial institutions about their customer‘s detailed information like their financial position and risk tolerance [1]. It includes verification of ID card, document verification for proof of address and biometric verification [2]. KYC helps in preventing money laundering, antisocial activities and other financial frauds. Manual KYC process followed by the banks currently suffers from increased cost, delay and redundancy [3] as shown in figure 1. On the other side automating KYC process may cause increase in cyber crime and will affect customer‘s privacy by exploiting the system. Newly emerging Blockchain Technology can be a solution to secure the KYC process due to its features like decentralization, immutability and trustlessness [4]. Blockchain is a distributed ledger technology, connecting number of peers together, where each peer maintains the copy of ledger on it [5]. These ledgers are immutable due to advanced cryptography techniques used in it [6]. Two major types of Blockchain are Public Blockchain and Private Blockchain. Public Blockchains are permissionless where anybody with essential resources can join the network while to join the private Blockchain network it is mandatory to take permission from admin of that Blockchain network. Bitcoin and Ethereum are the examples of Public Blockchain and Hyperledger Fabric is a well-known example of Private Blockchain [7]. Blockchain and Big data analytics are the most prominent technologies in present digital era and have been utilized successfully for several banking applications to facilitate the computerization [8, 9]. In this paper, we are utilizing Ethereum Blockchain platform to implement Blockchain based KYC verification system. Ethereum was developed in 2013 by Vitalik Buterin. Ethereum is a first Blockchain which has introduced concept of smart contract with which distributed apps (Dapps) can be created on top of the Blockchain [10]. Unlike Bitcoin, Ethereum could be used to develop different applications on top of it and is not limited as just payment alternative [11].The healthcare business can benefit from the Internet of Things (IoT) in terms of data management and transfer. Patient health data can be acquired locally from devices that can be used to make real-time decisions based on the data. For many years, several hospitals have deployed IoT in their patient rooms and their body parts. IoT devices could be vulnerable to hacking due to a lack of authentication and encryption policies, posing serious hazards to consumers. As a result, blockchain is useful for securing and proving transactions in the IoT.

As a result, it is proposed that the problem be solved using Fog Computing (FGC), Edge Computing, and blockchain. Based on FGC technology, models of analysis, and a signature-encryption algorithm (SE), a three-tiered architecture is employed for the identification, verification, and identification of healthcare IoT devices. The generated findings are used to assess the suggested innovative SE algorithm. We discovered that FGC-based blockchain performed better for detecting malicious nodes in terms of packet error rate, reliability, and throughput when compared to cloud settings and other environments. By 2025, healthcare IoT devices will account for 39% of total IoT devices [1]. ECGs and EEG monitoring are just two examples of time-sensitive applications in healthcare that must continuously evaluate reports from medical specialists and patient electronic health Data (PEHD) [2,3]. Currently, the IoT and medical devices communicate using a centralized model. It costs more to maintain and operate IoT devices connected to cloud servers. Data transmission is using a multiple hop count in the IoT-cloud environment shown in Fig. 1. Using routers between IoT and cloud is all that the conventional method involves. Cloud servers do not have the capacity to handle high volumes of IoT data, a major concern because of the centralized nature of cloud data management [4,5]. It needs to manage a distributed IoT ecosystem because of its centralized operation, risks of malicious attacks, and presents a single point of failure [6,7]. In IoT-based FGC cloud systems, blockchain is expected to resolve and overcome security and privacy concerns [8,9]. In addition, a blockchain-based system provides cryptographic functions with mining at the edge of a network. In [10], a cloud-based data framework is able to store the data using cryptography but it lacks the feasibility of adding components to the framework [11]. The author has experimented and proved that the latency of transactions is efficient in blockchain compared with cloud storage. Healthcare IoT devices typically transmit data to cloud servers without encryption, making them vulnerable to attack. As a result, sensitive information about patients may be compromised. Our study suggests that IoT-connected healthcare devices should be able to identify themselves with the possibility of healthcare data verification and authentication [10]. A novel blockchain-based IoT system is called Beekeeper [12]. Cloud servers can perform calculations on user data in the proposed system to process data. A node can serve as a server authorization leader if it has been selected by the current server authorization leader. Beekeeper has been deployed on the Ethereum blockchain. Parameters for users and miners were generated by the main authority. In [13], the authors used an encryption-based method to store and access the live streaming image data from sensors using a new model of Blockchain. In [14], the authors used encryption-based attributes in order to enable users to verify and decrypt them. We found the

technique useful for maintaining secure transmission in IoT. However, their proposal does not address the issue of identifying devices or authenticating keys. Using blockchain to integrate data and transmit it securely is what the authors did in [13]. The following sections of the paper are organized as follows: The second section discusses the related work. The proposed system's motivation is presented in Section 3. The background of blockchain architecture based on FGC is presented in Section 4. The proposed PEHD system is shown in Section 5. The evaluation of the experimental design is presented in Section 6. The final section highlights the result and discusses future work.

In ‗A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing,‘‘ Ciphertext-policy attribute-based encryption(CP-ABE) has been widely studied and used in access control schemes for secure data sharing. Since in most of the existing attribute-based encryption methods, all user attributes are managed by a single central authority, it is easy to cause a single point of failure. Therefore, several multi-authority CP-ABE schemes are proposed to manage user attributes by multiple authorities. However, these schemes still do not eliminate the single point of failure in essence or suffer from high computation and communication overhead on data users. In this paper, we propose a Blockchain-based Multi-authority Access Control scheme called BMAC for sharing data securely. Shamir secret sharing scheme and permissioned blockchain (Hyperledger Fabric) are introduced to implement that each attribute is jointly managed by multiple authorities to avoid single point of failure. In addition, we take advantage of blockchain technology to establish trust among multiple authorities and exploit smart contracts to compute tokens for attributes managed across multiple management domains, which reduces communication and computation overhead on the data user side. Moreover, blockchain helps to record the access control process in a secure and auditable way. Finally, we analyze the security of the proposed algorithm. Further analysis and comparison show the performance of the proposed method. With the development of Internet technology and technological innovation, the cloud has significantly changed the way data is shared. It provides individuals and industries with various data storage and management services that enable customers to easily access resources and share data. A Global Industry Vision (GIV) whitepaper predicts that, by 2025,―every company everywhere will be using cloud technology and 85% of business applications will be cloud-based‖[1]. While cloud providers put a lot of effort into ensuring the convenience of data sharing, there are still many security issues need to be considered. One of the main concerns is that cloud providers are not fully trusted. They will not only

suffer external attacks from adversaries, but also internal attacks from malicious staff, which leads to huge data security risks for data sharing in cloud. For example, Azure security vulnerability result in the disclosure of 250M Customer Details [2], Amazon employees leak customers‘ personal data to third parties for personal interests [3], and it is not uncommon for cloud storage providers to snoop on users‘ private data. To address the above issues caused by not fully trusted cloud storage service providers, cryptographic access control schemes such as IBE [4], CP-ABE [5] and KP-ABE [6] are proposed to secure sharing data by encrypting it with a secret key, such that only users with the secret key can decrypt data. Ciphertext-policy attribute-based encryption (CP-ABE) is considered as one of the most suitable technology to provide secure data access control in public cloud storage [7]. However, in most of existing CP-ABE schemes [7], [8], [9], all participants are forced to trust a single authority. It is easy to cause a single point of failure, and in practical applications, attributes are generally distributed across different trust domains and organizations. Therefore, Chase [10] propose the first multi-authority CP-ABE scheme, in which several disjoint domains are managed by different authorities to realize that user attributes are issued across multiple authorities. Although some extensions are also proposed [11], [12], [13], they still have the problem of the single-point of failure. Since in these schemes, the whole attribute set is divided into multiple disjoint subsets each of which is maintained by only a single authority. Li et al. [14] propose a TMACS scheme, taking advantage of threshold secret sharing to deal with the single-point bottleneck problem. Such that any one authority cannot obtain the master key by itself alone. Nevertheless, in this scheme, data users need to select multiple authorities from the authority list and communicate with each of these authorities to request secret key shares, which brings additional computational and communicational overhead. As a promising technology, blockchain has received much attention in recent years. Inspired by security properties of blockchain [15] and its innovative application in data communication [16], [17] and sharing [18], [19], [20], [21], [22], [23]. We intend to establish multi-party trust through blockchain, write the collaborative computing procedure among multiple authorities from multiple attribute domains into smart contracts, and generate decryption tokens for users. Since blockchain transactions have the property of transparency, it is necessary to consider how to integrate off-chain and on-chain algorithms to ensure the security of access control scheme based on blockchain. In this paper, we propose a blockchain-based multi-authority access control scheme, named BMAC, for secure cloud data sharing to address the issues mentioned above such as multi-authority cross-domain collaboration, single point of failure and high computational and communicational overhead.

In addition, a trustable and immutable access logs is recorded on blockchain, such that data owner can easily monitor users‘ access behavior. Overall, our main contributions are summarized as follows.

- A decentralized access control scheme based on blockchain and multi-authority attribute-based encryption, named BMAC, is proposed, which can solve the problems of a single point of failure, high computation and communication overhead on the data user side. In this scheme, the data access logs can be recorded on the blockchain, so as to realize auditable access control management.
- We extend the classical multi-authority attribute-based encryption method and design four smart contracts to realize multi-authority cross-domain collaboration. We take advantage of smart contracts to establish mutual trust between multiple authorities and collect attribute sub-tokens for collaborative calculations to generate a decryption token for users.
- We analyzed the security and performance of the scheme, and analyzed the effectiveness of our multi-authority ABE scheme from the perspective of communication overhead and computation overhead on the user side.

In __Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks,‘‘ Integrating blockchain into the Internet of Things (IoT) for security is a new development in computational communication systems. While security threats are changing their strategies and constructing new threats on blockchain-based IoT systems. Also, in combining blockchain with IoT networks, malicious transactions and active attacks deliver more vulnerabilities, privacy issues, and security threats. The concept of blockchain-based IoT attacks is a hot topic in both IoT and blockchain disciplines. Network attacks are a type of security and privacy threat and cover the exact scope of threats related to the combination of IoT and blockchain. Even though blockchain has potential security benefits, new cyberattacks have emerged that make blockchain alone insufficient to deal with threats and attacks in IoT networks since vagueness and ambiguity issues are unavoidable in IoT data. The heterogeneous nature of IoT sources has made uncertainty a critical issue in IoT networks. Deep Learning (DL) models have difficulty dealing with uncertainty issues and cannot manage them efficiently as an essential tool in security techniques. Thus, we need better security, privacy, and practical approaches, such as efficient threat detection against network attacks in blockchain-based IoT environments. Also helpful to consider fuzzy logic

to tackle deterministic issues when DL models face uncertainty. This paper designs and implements a secure, intelligent fuzzy blockchain framework. This framework utilizes a novel fuzzy DL model, optimized adaptive neuro-fuzzy inference system (ANFIS)-based attack detection, fuzzy matching (FM), and fuzzy control system (FCS) for detection of network attacks. The proposed fuzzy DL applies the fuzzy Choquet integral to have a powerful nonlinear aggregation function in the detection. We use metaheuristic algorithms to optimize the attack detection error function in ANFIS. We also validate transactions via FM to tackle fraud detection and efficiency in the blockchain layer. This framework is the first secure, intelligent fuzzy blockchain framework that identifies and detects security threats while considering uncertainty issues in IoT networks and having more flexibility in decision-making and accepting transactions in the blockchain layer. Evaluation results verify the efficiency of the blockchain layer in throughput and latency metrics and the intelligent fuzzy layer in performance metrics (Accuracy, Precision, Recall, and F1-Score) in threat detection on both blockchain and IoT network sides. Additionally, FCS demonstrates that we obtain an effective system (stable model) for threat detection in blockchain-based IoT networks. The Internet of Things (IoT) is one of the fastest growing technologies. It is undeniable how important and applicable IoT has become in our everyday lives. IoT turns any device through its existing network infrastructure empowering physical resources into intelligent entities. IoT networks aim to develop a complex information system with sensor data acquisition and efficient data exchange through networking, artificial intelligence (AI), machine learning (ML), clouds, and big data (Barrios et al., 2022, Yazdinejad et al., 2020c). At this time, due to ever-growing security threats, malicious attacks, and criminal activities, investigating cyber-attacks has become a critical issue, especially in IoT environments. IoT security is an ongoing concern since IoT networks and applications leave plenty of room for hacking. This lack of security can be a real concern when considering IoT networks in financial tasks, smart homes, and smart car applications. Many industrial sectors and organizations utilizing IoT networks seek solutions to enhance their security. In this regard, there are many security recommendations for IoT networks. One well-known and potential security solution in IoT networks is blockchain. Blockchain has been integrating with IoT, especially in network design, financial transactions, device authentication, and identification (Wu et al., 2022).

Applying blockchain in IoT is necessary since the IoT architecture is centralized and applies a third-party central authority. The central authority controls all data without imposing clear restrictions on its use (Da Xu et al., 2021). On the other hand, blockchain technology delivers a decentralized, autonomous, trustless, and distributed environment. Unlike centralized

systems, which have problems with single points of failure, trust, and security, blockchains use the processing capacities of all the participating users, providing greater efficiency and eliminating the single point of failure. Furthermore, blockchain offers better security and data integrity due to its immutable and unchangeable features. In computational communication systems, the integration of blockchain and IoT are essential developments (Šarac et al., 2021). Blockchain and IoT both have the meaning of connection and are two dimensions of the information processing system. At this time, we have been faced with a blockchain-based IoT concept. Based on IBM‘s definition, IoT enables devices via the internet to forward data to the blockchain to create immutable records of transactional data in blockchain-based IoT systems. Blockchain as a service layer is considered a layer between the application and network layers in the typical IoT architecture. Several blockchain IoT projects have influenced the business and industry such as IoTA, Waltonchain, IoTex, Ambrosus, Moeco, and Atanomi. Also, we can mention some real-world implemented blockchain-based IoT items such as Telstra, Mediledger, NetObjex, Slock.it, and Drone on the Volga. Despite the potential blockchain security benefits in IoT, there are significant cyberattacks on IoT networks seen when applying blockchain. Also, security issues are still a significant concern for blockchain-based IoT systems due to the vulnerabilities of IoT and blockchain. Depending on the characteristics of the blockchain, attackers change their strategies and construct new attacks on blockchain-based IoT system (Da Xu et al., 2021). There are some blockchain-based IoT security attacks, including distributed denial-of-service (DDoS), injection, abandon, denial-of-service (DoS), falsifying, public block modification, link modification, and time interval destruction (Da Xu et al., 2021). To explain some blockchain-based IoT attacks, Abandon is an auditing node that discards its members‘ transactions and isolates them, DoS is the target node by sending too many transactions to it, exceeding its processing capabilities, DDoS attacks use more than one node, Equipment Injection allows an attacker to gain unauthorized access to private data by injecting a fake node into the network, and Link, by using the same ID, the attacker can find real-world identifiers corresponding to anonymous nodes. As a real example, IOTA was attacked by DDoS and Trinity (IOTA, 2020). Therefore, blockchain alone is not enough and cannot be a complete security solution to tackle intrusion attacks and make valid transactions on IoT networks. Intrusion attacks and fraud transactions on IoT networks have grown exponentially at the device level. Malicious actors threaten IoT networks by malicious transactions in blockchain Singh et al. (2020b). They can attempt to determine a particular user by finding links between the user‘s anonymous transactions and other publicly available information. Malicious transactions

have behavioral patterns and even show different patterns during various attacks. Malicious actors can also attempt to pass themselves off as legitimate users to gain access to data. Also, in addition to some common attacks in blockchain (such as 51% attacks, eclipse attacks, Sybil attacks, Finney attacks, decentralized autonomous organization (DAO) attacks, DDoS race attack, and routing attack (Aggarwal and Kumar, 2021, Anon, 2021)), we can mention some recent ways that they have exposed vulnerabilities and attacks in blockchain-based IoT networks. Active attacks, like, jamming and impersonation, are emerging on blockchain due to multiple active malicious nodes (Mujtaba Buttar et al., 2022). These active attacks lead to the failure of the consensus process responsible for verifying the transactions in the blockchain. In addition, a spam Destination Oriented Directed Acyclic Graph (DODAG) Information Solicitation (DIS) attack is a novel attack that consumes the energy of IoT devices in blockchain frameworks, resulting in a Denial of Service (DoS) vulnerability (Alsirhani et al., 2022). These attacks prove that IoT devices and networks are vulnerable to security threats, and blockchain is not a sufficient safeguard for IoT security (Yazdinejad et al., 2022a). According to IoT security taxonomy based on blockchain networks (Da Xu et al., 2021), there are mainly two types of threats in blockchain-based IoT systems. First, blockchain-related privacy threats in the blockchain layer. Second, IoT security threats in the IoT layer. Hence, network attacks are a type of security and privacy threat related to IoT and blockchain. In this paper, network attacks cover both threats in both IoT and blockchain, especially the most prominent attacks in this regard, including Denial of Service (DoS), probing, Remote to Local (R2L), transaction privacy leakage, and phishing (Bahaa et al., 2021). Another challenge we should mention here is the uncertainty and vagueness of data issues in IoT networks that are unavoidable (Yazdinejad et al., 2020b). Taking into account the heterogeneous nature of IoT sources, uncertainty has become a vital issue in IoT networks since data may not be measured accurately or capable of being understood in either of two or more possible senses. At the same time, DL models are widely used in security techniques since they can efficiently process any piece of information in the cybersecurity datasets by defying attacks. However, DL models have difficulty dealing with uncertainty issues. They cannot manage uncertainty issues efficiently, while blockchain-based IoT networks need more security and practical approaches, such as efficient threat detection. In both IoT and blockchain research, the blockchain-based IoT attack area is a hot topic, and we need to tackle the security threats in this area more effectively. As a result, it is a more pressing concern to consider practical security approaches such as efficient threat detection in blockchain-based IoT networks. Due to ever-rising security threats in IoT

networks (Singh et al., 2020b, Yazdinejad et al., 2020c) while applying blockchain and its benefits, our motivation has been formed to provide an effective security approach in blockchain-based IoT networks. Our main innovation is designing and implementing a secure intelligent fuzzy blockchain framework that can effectively detect security threats in IoT networks while providing more efficiency in the blockchain layer. We apply deep learning (DL) and fuzzy logic concepts in this framework. DL has shown good performance in improving cybersecurity attack detection, and it is a critical part of modern cybersecurity strategies. DL also is capable of analyzing attack patterns and learning to prevent similar attacks and respond to changing behaviors. The fuzzy logic approach can help make reasonable decisions concerning threat detecting and makes DL works with indeterministic assumptions (Makkar et al., 2021) in IoT networks that utilize blockchain.

In ‗High-frequency trading on decentralized on-chain exchanges,‖ Decentralized exchanges (DEXs) allow parties to participate in financial markets while retaining full custody of their funds. However, the transparency of blockchain-based DEX in combination with the latency for transactions to be processed, makes market-manipulation feasible. For instance, adversaries could perform front-running — the practice of exploiting (typically non-public) information that may change the price of an asset for financial gain.In this work we formalize, analytically exposit and empirically evaluate an augmented variant of front-running: sandwich attacks, which involve front- and back-running victim transactions on a blockchain-based DEX. We quantify the probability of an adversarial trader being able to undertake the attack, based on the relative positioning of a transaction within a blockchain block. We find that a single adversarial trader can earn a daily revenue of over several thousand USD when performing sandwich attacks on one particular DEX — Uniswap, an exchange with over 5M USD daily trading volume by June 2020. In addition to a single-adversary game, we simulate the outcome of sandwich attacks under multiple competing adversaries, to account for the real-world trading environment. Decades of asset trading on traditional exchanges have brought to fruition a veritable collection of market manipulation techniques, such as front-running [6], pump and dump schemes [54] and wash trading [3]. In the context of cryptocurrencies, research to date indicates that the ecosystem requires a greater awareness of such malpractices [54], [21], [45], and better exchange design [12] to prevent misbehavior. Most existing legislation does not regulate crypto-exchanges to the same degree as traditional exchanges — leaving ignorant traders open to exploitation by predatory practices, some of which is close to risk-free. Decentralized exchanges (DEXs)

allow traders to trade financial assets without giving up asset custody to a third party. Orders can be placed and matched in their entirety through immutable blockchain smart contracts, offering the possibility of censorship resistance, where orders cannot be modified prior and after execution Censorship-resistant trade is itself made possible through reliance on an underlying blockchain, which makes public all attempted and executed trades within its peer-to-peer (P2P) network. The transparency of the blockchain layer, however, in combination with the latency for orders to deterministically execute makes, front-running easier to undertake — and hence influences negatively the security of the trader‘s assets. This paper. We focus on a combination of front- and back-running2 , known as a sandwiching, for a single onchain DEX. To the best of our knowledge, we are the first to formalize and quantify sandwich attacks. To make their sandwich, a predatory trader first observes a blockchain P2P network for a victim transaction and then rushes to squeeze it by placing one order just before the transaction (i.e. front-run) and one order just after it (i.e. back-run). If the target transaction is going to increase (decrease) the price of an asset, the adversary can place an order before which buys (sells) the asset in question, and an order afterward which sells (buys) the asset again. We restrict our focus to automated market maker (AMM) DEXs [52], [4], as opposed to DEXs which operate limit order books (LOB) [20], on account of their deterministic nature which enables us to rely on fewer assumptions in our analysis. AMM DEXs simplify trading by algorithmically performing market making3 , resulting in nearinstant liquidity (i.e. the ability to purchase and sell assets) for market participants. Uniswap is a prominent example of an AMM DEX, which, by March 2020, has amassed a total liquidity of nearly 48M USD (corresponding to a 75% market liquidity share for AMM DEX) and had a trading volume of over 250M USD since its inception in November 2018. We formalize, analytically exposit and empirically evaluate sandwiching on AMM DEXs. We quantify optimal adversarial revenues and perform a realworld empirical evaluation of sandwich attacks. We also study the probability of a transaction having a particular relative position within a blockchain block, informing the prospects for such an attack. Finally, to account for a realworld scenario in which multiple adversaries are likely to 2While the SEC defines front-running as an action on private information, we only operate on public trade information. 3The process of serving a market with the possibility to purchase and sell an asset. compete over victim transactions, we perform simulations to quantify the transaction fees resulting from a reactive fee counter-bidding contest.

2. MATERIALS AND METHODS:

The exponential growth of digital infrastructures like the cloud and the IoT has resulted in the accumulation of massive amounts of personally identifiable information. Users and businesses alike get enormous financial rewards from the information society as a result of the persistent collection and analysis of personal data by corporations, who in turn provide users expert services and create substantial economic advantages. There has been a disturbing uptick in the number of cases of personal data leaking in recent years due to businesses' lax data security practices, such as keeping data in unencrypted on their central servers. Consequently, it is essential to securely share and store private data. Blockchain, a distributed ledger database, offers a trustworthy environment for data storage and exchange thanks to its decentralized nature and the difficulty in tampering with data. Data storage, the IoT, healthcare, transactions, and payments are just a few areas where blockchain technology is now being tested by academics. Meanwhile, tamper-resistant ledger databases have been the subject of much academic inquiry. Any user may access data information stored on the blockchain unless the data owner specifically keeps information linked to private data elsewhere. Because of this, the data owner can end up with no control over their data. The approach put out by Bethencourt is Ciphertext-PolicyAttribute-Based Encryption, or CP-ABE. The data owner has the option to choose the ciphertext access method in CP-ABE. This approach encrypts the data with the access policy and embeds the user attribute defined in the key.

Problem with the Current System • High Level of Complexity and Computational Expenses: Computational overhead increases when dealing with high-dimensional attribute domains because of the complexity of the methods and calculations needed. The system's efficiency and resource consumption could be negatively impacted by its complexity. • Key Management: Key management is a crucial component of many encryption methods, particularly when dealing with revocation. Properly managing keys for high-dimensional qualities is essential to avoid security risks caused by onerous and complex management. Problems with the system's scalability may arise as the amount of characteristics and dimensions grows. System performance and efficiency may suffer if a huge number of characteristics are handled.

• User Experience: The ease of usage may be compromised by intricate encryption and revocation procedures. User confusion and reluctance to utilize the system properly might result from too complicated procedures.

PROPOSED SYSTEM • ABE, or Attribute-based Encryption, encrypts data depending on a number of characteristics. Use ABE with ciphertext or key policies to provide access control

based on combinations of attributes. Secure processing without decrypting sensitive information is possible with the help of homomorphic encryption, which allows calculations to be performed on encrypted data. Securely produce, store, and distribute keys with the help of a solid key management system. Key revocation nd update techniques should be supported by this system efficiently. You may enable dynamic revocation of characteristics or combinations of attributes without jeopardizing the whole encryption scheme.

3. DISCUSSION

• Encrypt information by using a mix of characteristics. Make use of ABE methods (such as ciphertext-policy or key-policy) to grant access depending on certain combinations of attributes.

• Decrypt the data using the properties of the user's private key and the encrypted data itself. You need to check the user's characteristics against the data's access regulations to make sure they have the right ones to decrypt. The Benefits • Improved Data Security: The system enables fine-grained control over who may access what sensitive data by limiting decryption to individuals with certain traits or combinations of features.

• Fine-Grained Access Control: It allows for fine-grained access control, which improves data security by limiting user access to just the properties they are permitted to see or change.

• Decreased Security Risks: Sensitive information stays protected and out of the reach of unauthorized users thanks to advanced encryption methods, greatly reducing the danger of data breaches and unlawful access.

SYSTEM ARCHITECTURE

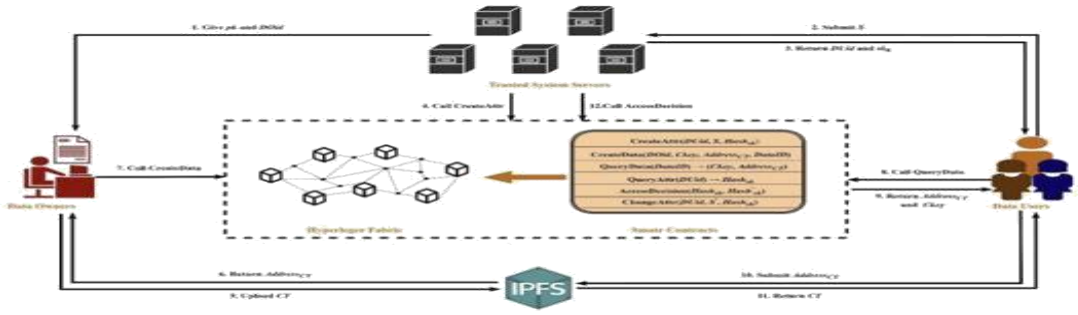


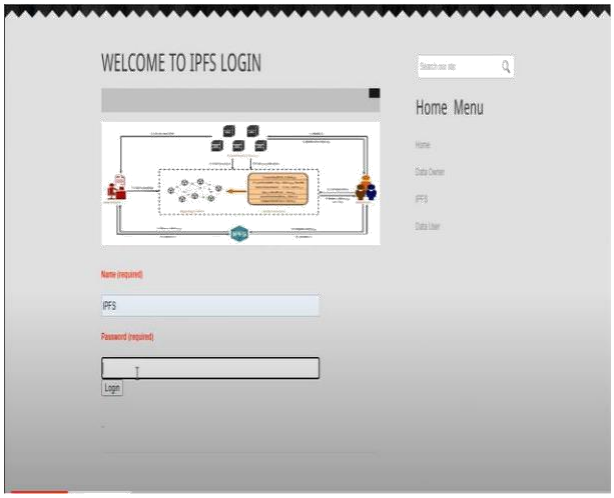
Fig1: system overview

Owner of Data He enters his credentials (username and password) to access this section. Once logged in, the data owner may proceed to do the following: Create an Account and Access It, Feel free to upload and see any dataset you want. Individual Using Data He enters his credentials (username and password) to access this section. The user will be able to access many functions after logging in, including the following: register and login, request call attributes, see all request statuses, and find details of call attributes. Servers for the Trusted System The trusted system servers are able to do tasks like logging in and seeing attributes using this module. IPFS In addition to storing data, the IPFS server also allows users to perform things like log in, see who owns the data, see who uses the data, see all datasets, and sort datasets by blockchain. You may check the status of all attribute requests, see who has been revoked access, see the results of all calls, and see the titles of all calls.

4. RESULTS

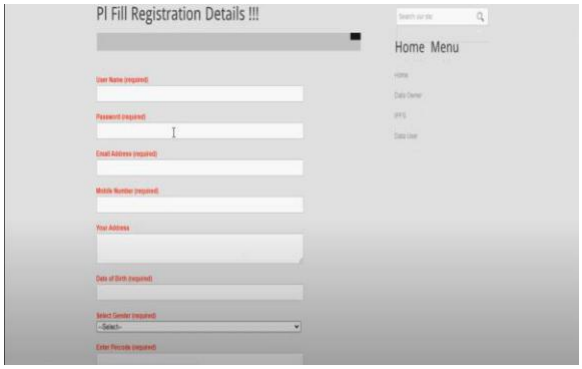
HOME PAGE

IPFS LOGIN PAGE



Enter Valid Credentials For login Purpose

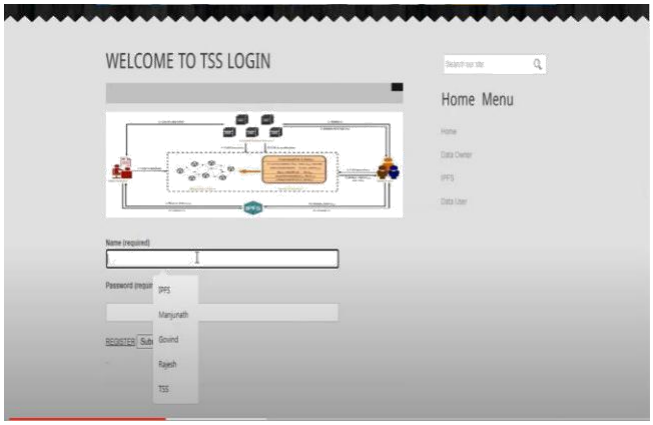
DATA OWNER REGISTRATION PAGE



After Passing the Required Values in the field for Registration

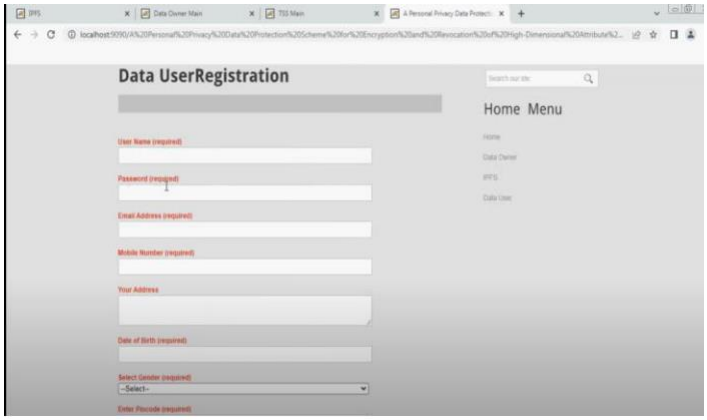
Purpose LOGIN PAGE

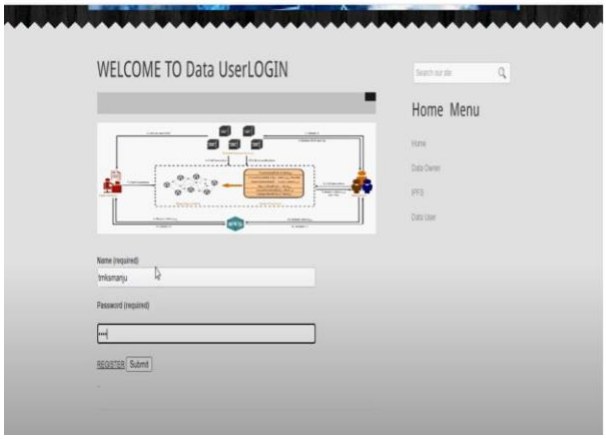
Registration is Completed Activate the User after activation login with that credential TSS LOGIN PAGE



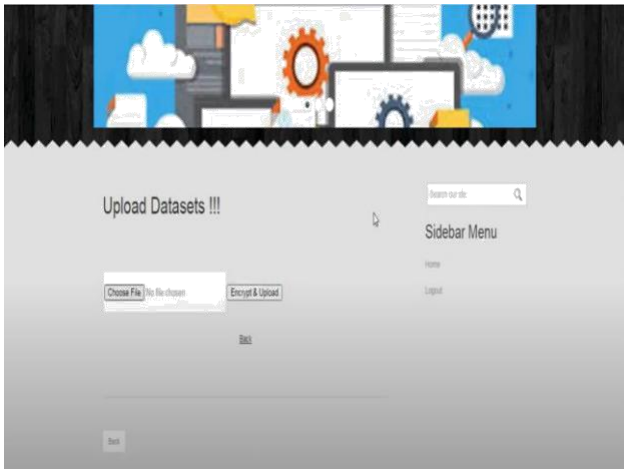
Enter Valid Credentials For login Purpose

DATA USER REGISTRATION PAGE



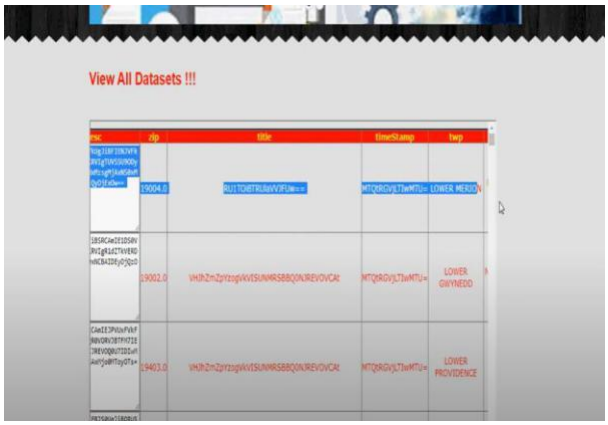


Registration is Completed Activate the User after activation login with that credential UPLOAD DATA SET

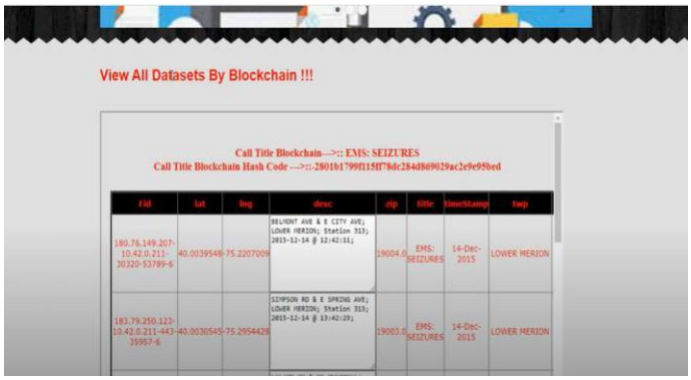


Upload Data after Encrypting

VIEW ALL DATA SETS



VIEW ALL DATA SET BY BLOCK CHAIN



5. CONCLUSIONS

Current techniques in high-dimensional attribute domains have poor security, substantial computational overhead, and high attribute revocation cost; to solve these difficulties, we have presented a personal privacy data protection strategy for encryption and revocation of these domains. In high-dimensional attribute domains, safe data storage and exchange is

essential, and HAD-FME, built on top of FAME and SM4 with strong security, can do this while reducing processing overhead. In addition, we developed SM-ARM, an Attribute Revocation Mechanism Based on Sentry Mode, to lessen the burden of attribute revocation via limited key updates to the user. In this research, we have presupposed that STSS cannot acquire a full DU private key and that the blockchain system displays performance constraints. To further increase the speed and throughput of privacy data protection schemes, we want to investigate multi-authority-based key generation methods that guarantee DU security in the future. These schemes will be built on high-performance tamper-proof systems.

6. **REFERENCES AND CITATION**

[1] P. Patil and M. Sangeetha, __Blockchain-based decentralized KYC verification framework for banks,‘‘ *Proc. Comput. Sci.*, vol. 215, pp. 529–536, Jan. 2022, doi: 10.1016/j.procs.2022.12.055.

[2] V. Mani, M. M. Ghonge, N. K. Chaitanya, O. Pal, M. Sharma, S. Mohan, and A. Ahmadian, __A new blockchain and fog computing model for blood pressure medical sensor data storage,‘‘ *Comput. Electr. Eng.*, vol. 102, Sep. 2022, Art. no. 108202, doi: 10.1016/j.compeleceng.2022.108202.

[3] X. Qin, Y. Huang, Z. Yang, and X. Li, __A blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing,‘‘ *J. Syst. Archit.*, vol. 112, Jan. 2021, Art. no. 101854, doi: 10.1016/j.sysarc.2020.101854.

[4] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, __Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks,‘‘ *Comput. Ind.*, vol. 144, Jan. 2023, Art. no. 103801, doi: 10.1016/j.compind.2022.103801.

[5] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, __High-frequency trading on decentralized on-chain exchanges,‘‘ in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 428–445, doi: 10.1109/sp40001.2021.00027.

[6] E. Androulaki et al., __Hyperledger fabric: A distributed operating system for permissioned blockchains,‘‘ in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[7] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, __LedgerDB: A centralized ledger database for universal audit and verification,‘‘ *Proc. VLDB Endowment*, vol. 13, no. 12, pp. 3138–3151, Aug. 2020, doi:10.14778/3415478.3415540.

[8] C. Yue, T. T. A. Dinh, Z. Xie, M. Zhang, G. Chen, B. C. Ooi, and X. Xiao, __GlassDB: An efficient verifiable ledger database system through transparency,‘‘ *Proc. VLDB Endowment*, vol. 16, no. 6, pp. 1359–1371, Feb. 2023, doi: 10.14778/3583140.3583152.

[9] J. Bethencourt, A. Sahai, and B. Waters, __Ciphertext-policy attributebased encryption,‘‘ in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334, doi: 10.1109/SP.2007.11.

[10] S. Agrawal and M. Chase, __FAME: Fast attribute-based message encryption,‘‘ in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 665–682, doi: 10.1145/3133956.3134014

[11]. P. Patil and M. Sangeetha, "Blockchain-based decentralized KYC verification framework for banks", *Proc. Comput. Sci.*, vol. 215, pp. 529-536, Jan. 2022.

[12]. V. Mani, M. M. Ghonge, N. K. Chaitanya, O. Pal, M. Sharma, S. Mohan, et al., "A new blockchain and fog computing model for blood pressure medical sensor data storage", *Comput. Electr. Eng.*, vol. 102, Sep. 2022.