IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 5, Issue 6, June 2025

Impact Factor: 5.731

An Authorized Scheme Service Privately Shared Data

Bandari Ravi[1], Kunaal KT[2], M. Achyuth[3], K. Sai Krupal[4]

Assistant Professor, Department of Computer Science & Engineering[1]

Students, Department of Computer Science & Engineering[2,3,4]

Guru Nanak Institute of Technology, Hyderabad

Abstract: *In the modern digital landscape, the secure sharing of data across distributed systems remains a critical challenge. This paper proposes a blockchain-based architecture that leverages publicly verifiable proxy re-encryption to enable secure and controlled data sharing between users without exposing the underlying plaintext to unauthorized entities or intermediaries. The system is divided into three primary modules, each hosted on a separate server, to enhance security, scalability, and modularity. Server 1 is responsible for storing encrypted data and generating the corresponding private keys. It also performs the initial encryption and re-encryption processes to prepare data for secure sharing. Server 2 manages user file requests, verifies user permissions, and facilitates key distribution. Upon receiving a request, Server 2 checks whether the user has the right to access the file and provides the required key if the request is approved. Server 3 plays a crucial role in user registration, login, and access management. It supports multiple user requests, ensuring that each user's identity and access rights are properly handled. The second part of the system focuses on user-level interactions. Users must register and log into the system before they can upload data, search for existing data, or request access to encrypted files. Once registered, users can view the encryption keys associated with their data and request re-encryption keys for sharing information securely with other users. At the core of this architecture lies the publicly verifiable proxy re-encryption scheme. This cryptographic approach includes several key algorithms: key generation (KeyGen), encryption (Enc), re-encryption key generation (RkGen), re-encryption (ReEnc), verification of re-encrypted ciphertext (VerRe), and decryption (Dec). The KeyGen algorithm generates public-private key pairs for each user. With Enc, data is encrypted using the public key, and RkGen allows the data owner to produce a re-encryption key that permits a proxy to convert the ciphertext for another authorized user without revealing the plaintext. The ReEnc function transforms the ciphertext using this re-encryption key, while VerRe ensures that the transformation was correctly performed. Finally, Dec allows the intended recipient to decrypt the data using their private key. This framework ensures that only authorized users can access sensitive data, and the re-encryption process does not compromise confidentiality. Moreover, by distributing roles across three servers and employing blockchain for record-keeping and trust verification, the system achieves a high degree of transparency, traceability, and tamper-resistance. Proxy re-encryption plays a pivotal role in enabling dynamic and secure data sharing.*

Keywords: *digital landscape*

I. INTRODUCTION

There has been increased focus on user privacy, particularly due to the number of high profiles 'scandals' alleging data abuse or leakage. For example, it was alleged that a major social media platform provided personal data of its users to other organizations around the world for several years, according to the New York Times. This topic has also attracted the attention of policy-makers, such as the 'S.1667 - Social Media Privacy Protection and Consumer Rights Act of 2021' introduced by U.S. Senator Klobuchar in May 2021. However, regulation on its own is insufficient. Services through direct ciphertext computing (e.g., homomorphic encryption [6], secure multi-party computation [7], and trusted execution environment [8]) may not be practical due to a broad range of reasons, such as computational overheads or

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 6, June 2025
Impact Factor: 5.731

user inconvenience (e.g., due to the use of encryption). Even though some practical schemes based on the above technologies [9], [10], [11], [12], [13], [14] have been proposed, most of them have limitations (e.g., apply to narrow scenarios or inability to handle complex services). Therefore, it is very difficult and almost impossible for service providers to provide general services through crypto state calculations, the service provider access to plaintext for service is inevitable. In addition, there are legitimate reasons why service providers need to collect and exchange user information, such as to provide single sign-on [15] and other authentication services for a seamless user online experience. Therefore, we focus on minimizing information available to service providers and dependence on service providers, in order to mitigate any potential risks of data leakage problem due to the indiscriminate collection by service providers. An important source of data acquisition and analysis for service providers is the use of platform data by users, such as authorization, cross-platform use, etc., thereby generating the derived value of the data. The OAuth 2.0 protocol is widely used by service providers since it allows third-party applications (e.g., data receiver) to obtain specific resources stored by the resource owner (e.g., user) at the service provider (e.g., data source) [16]. This protocol is a centralized authentication protocol that relies on the authenticity of the data source (e.g., service provider).

II. LITERATURE SURVEY

Q. Huang, G. Yan, and Q. Wei discussed in their paper that access control plays an important role in cloud computing. Existing access control solutions mainly focus on preserving confidentiality of stored data from unauthorized access and the storage provider. A major challenge for accessing the outsourced data is the ability to deal with those requests for resources according to the specified security policies to achieve confidentiality while protecting the users' privacy. In this paper, we survey five privacy-preserving access control schemes from the views of privacy preserving of policy-hiding, user information, identity attribute, access policy, access pattern, DAC separately. Core techniques of each scheme are detailed. Security and privacy aspects on the proposed schemes are discussed.

C. Ge, W. Susilo, Z. Liu, J. Xia, P. Salchows, and L. Fang discussed in their paper that the shortcomings of conventional healthcare systems are becoming more apparent as the Internet of Things (IoT) becomes ever more pervasive in people's daily lives. The standard procedure for dealing with confidential data frequently results in unwanted public disclosure. Blockchain's agreements make it possible to automate the safe transfer of patient data based on their individual authorization settings. To create a completely untraceable trading platform, blockchain technology is frequently implemented. To protect user data in the Internet of Things (IoT), a privacy-protecting protocol is developed using the blockchain. It is important to consider that the rogue cloud server might potentially develop a database of user behavior profiles, which could be a serious breach of privacy. Confidentiality makes it more difficult to resolve disagreements about private data exchange transactions. When users of metadata are falsely accused, their rights are difficult to defend. Also, smart contracts are used to enforce security protocols and data privacy for multi sharing adaptable access control. There is no reason to doubt the safety of the proposed work. The proposed work is efficient and applicable, as demonstrated by the efficiency evaluation and experimental findings.

J. Wang and S. S. Chow discussed in their paper that Web3 is the evolution of internet requisites decentralized identity management known as a new paradigm in the identity management system. Web3 conceptualizes decentralization and based upon that needs an identity model that fulfills the requirement of any business/technology model in the new trusted third-party free era. This article presents Web3, Web3 architecture, and technologies expansion for secure and scalable services. Further, the decentralized identity management model is presented with its components (DID), reusable verifiable credentials (VC), issuer, verifier, and user centricity in perspective with the Web3 identity model.
M. W. Zhang, W. X. Song, and J. X. Zhang discussed in their paper that federated learning is proposed as an approach that enables several participants to collaboratively train the machine learning model, but without directly expose the local data to others. Although federated learning is developed to prevent the participants' local sensitive data leakage. However, recent researches show that federated learning systems are still faced with privacy and security challenges. In the privacy view, if participants or the central server are curious, they can inference information about the training data or the model by the exchanged update parameters. From a security perspective, the malicious participants can make

poisoning attacks during the model training phase. Differential privacy and security multiparty computation (SMC) is exploited to solve the privacy problem. But they often result in large communication overhead or low federated learning accuracy. Besides, there lacks a comprehensive scheme that has effects on both privacy and security issues. In this article, we proposed a homomorphic encryption-based privacy enhancement mechanism which has effectiveness on membership inference attacks. Our method works in two phases. In phase I, our method exploits homomorphic encryption to encrypts participants' update parameters before sending out to the aggregator. In phase II, we add a parameter selection method to the aggregator of the federated learning system to choose participants' updated information with a certain probability. The experimental results show that the proposed method effectively defends both against membership inference attacks and poisoning attacks and makes less model accuracy effects than other existing solutions.

K. Lee published their paper stating The Internet of things (IoT) technology has been used in a wide range of fields, ranging from industrial manufacturing to daily lives. The IoT system contains numerous resource-constrained lightweight devices such as wireless sensors and radio frequency identification (RFID) tags. A massive amount of sensitive data is generated and transmitted by these devices to a variety of users. The complexity of the IoT system places a high demand on security. Therefore, it is necessary to develop an encryption scheme with access control to provide flexible and secure access to the sensitive data. The ciphertext policy attribute-based encryption (CP-ABE) scheme is a potential solution. However, the long ciphertext as well as the slow encryption and decryption operations in traditional ABE schemes make it inappropriate for most IoT systems, which require low latency and contain many devices with limited memory size and computing capability. In this paper, we propose a modified CP-ABE scheme with constant length of ciphertext and low computation overhead in the encryption and decryption phases. Additionally, our scheme is proven to be adaptively secure under the standard model. Moreover, two enhanced schemes are developed to prevent authorized users from leaking data and protect the privacy of data owners by combining chameleon hash, bloom filters and CP-ABE, respectively. Finally, the experimental evaluation and analysis prove the feasibility of our scheme.

III. METHODOLOGY

The study of this paper is to understand the zero-knowledge proof allows the verifier to determine whether the prover's statement is correct (e.g., knowing a key piece of information) without revealing the information itself. A zero-knowledge proof system should satisfy completeness (i.e., the prover can convince the verifier that a statement is correct), reliability (i.e., if the statement is false, the cheating prover cannot convince the verifier), and zero-knowledge (i.e., protocol interactions only reveal whether a statement is correct and do not reveal any other information). We adopt the widely used zero-knowledge succinct noninteractive argument of knowledge (zk-SNARKs) in our work.

DISADVANTAGES OF EXISTING SYSTEM:

- No security authentication.
- It is not secure enough.
- Highly inefficient.

PROPOSED SYSTEM

There are privacy implications when users authorize share personal data managed by service providers. To make authorization private and controllable, in this paper, we propose a private authorization scheme-oriented service provider. A publicly-verifiable re-encryption method based on IPFS is proposed to minimize the on-service providers, by shifting to a distributed storage and computation model.

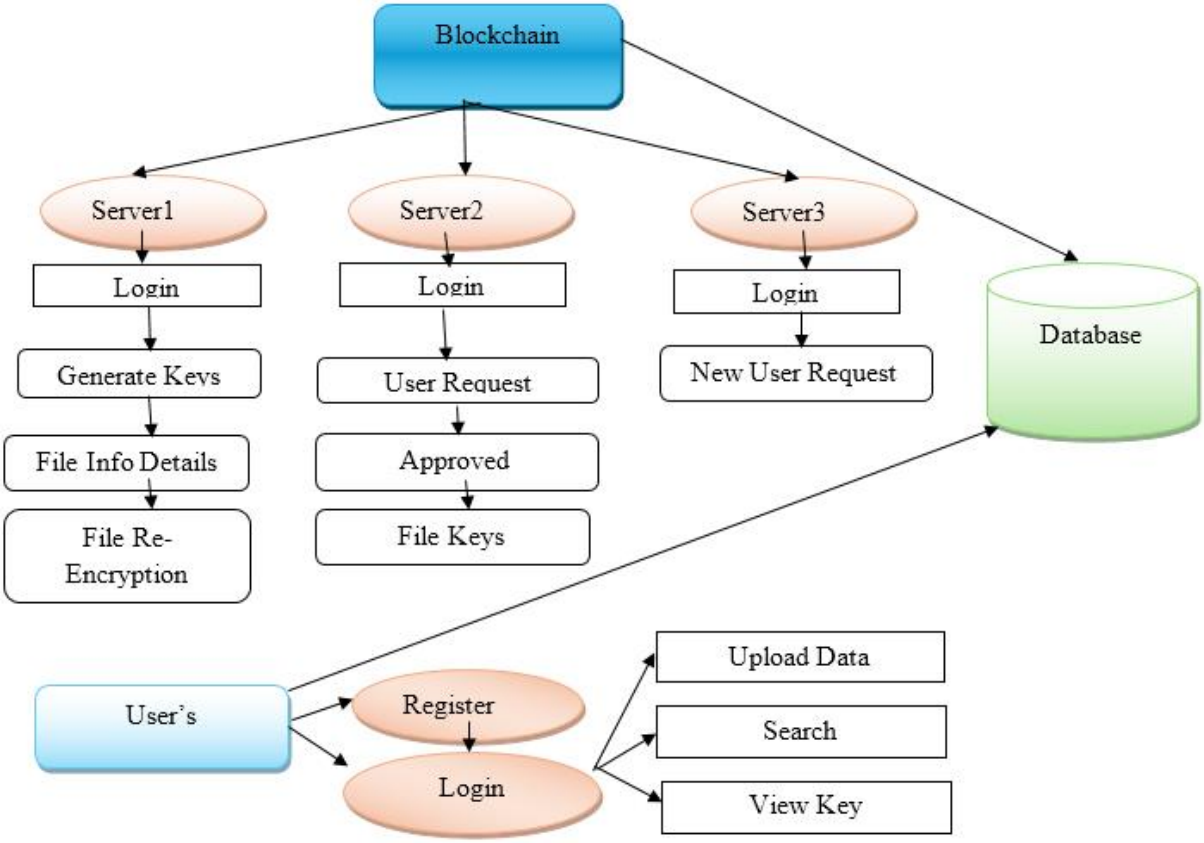
Besides, we propose a trustless authorization authentication method that hides the authorization relationship to protect user privacy.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 6, June 2025
Impact Factor: 5.731

ADVANTAGES OF PROPOSED SYSTEM:

- PRE schemes enable secure data sharing between parties without requiring the data owner to be online
- PRE schemes can be more efficient than traditional public-key encryption schemes in certain scenarios

SYSTEM ARCHITECTURE:



MODULES:

User Interface Design: In this module we design the windows for the project. These windows are used for secure login for all users. To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page.

Blockchain: This is the second module block chain. The blockchain divided with three servers. Server1,Server 2 and Server 3. Server 1 is for a storage data and it will generate a private key and it will convert a re-encryption. Server 2 has Users file Requests and searched file request it will get a server2 approved a key. Server2 has get a file keys. Server 3 is providing user to two users requests. For adding a user's file and downloading it.

User: This is the third module of this project the user has a register and then login. The user has an upload a data. The user has searched a data. The user has a view keys.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 6, June 2025
Impact Factor: 5.731

IV. IMPLEMENTATION

DATA ACCESS SERVLET:
Handles access to encrypted file data based on file ID (fid) and a provided master key (mkey). It verifies the key and decrypts the content if the key length is 16 characters and matches the stored data. Redirects to a data access page if successful, else to an error page.

RE-ENCRYPT DATA SERVLET:
Performs re-encryption of existing encrypted files. It retrieves file data using fid, generates a new 16-character encryption key, updates the database with the new key, and forwards the result to a JSP with the new encryption key and file details.

RANDOM KEY GENERATOR:
Generates a random alphanumeric string of a specified length. Used for generating new encryption keys during re-encryption.

RE-ENCRYPT KEY VERIFICATION:
Validates the correctness of the old and newly re-encrypted keys for a specific file. It compares submitted keys against expected values (placeholder logic) and forwards the result to a JSP indicating access approval or denial.

FILE SEARCH FUNCTIONALITY:
Implements a search feature that allows users to search files by name. Retrieves file information from the database and forwards it to a JSP for display.

SERVER LOGIN SERVLETS:
These servlets handle login logic for four different servers (Server, Server1, Server2, Server3). Each verifies a hardcoded password and redirects the user to their respective home JSP page or back to the login page if the password is incorrect.

ENCRYPTION UTILITIES
Provides utilities for AES encryption and decryption using CBC mode and Base64 encoding. Includes methods to generate 256-bit AES keys, encrypt plaintext, and decrypt ciphertext using a given key and IV. Also contains a main() method to demonstrate its usage.

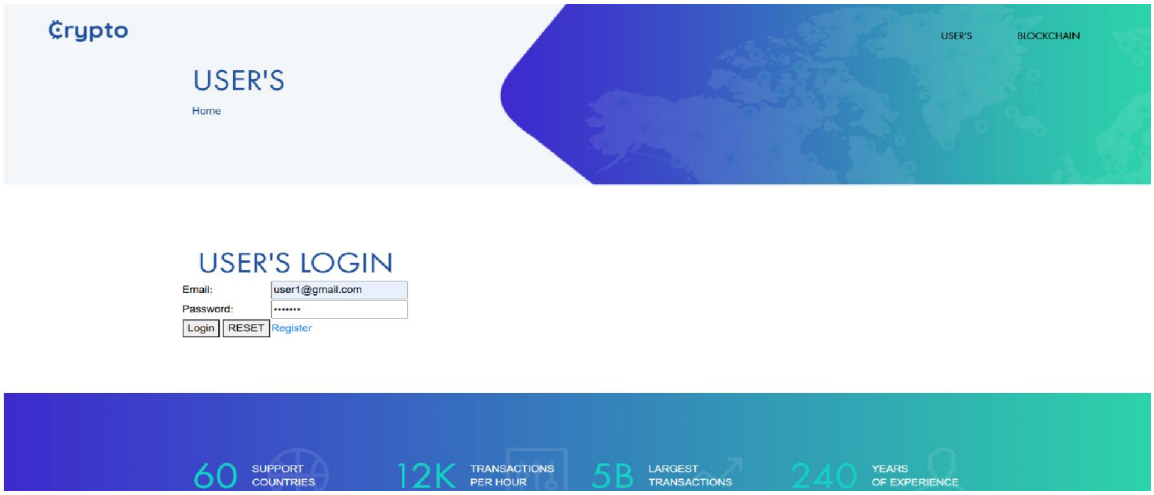
V. EXPERIMENTAL RESULTS

HOME PAGE

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 6, June 2025
Impact Factor: 5.731

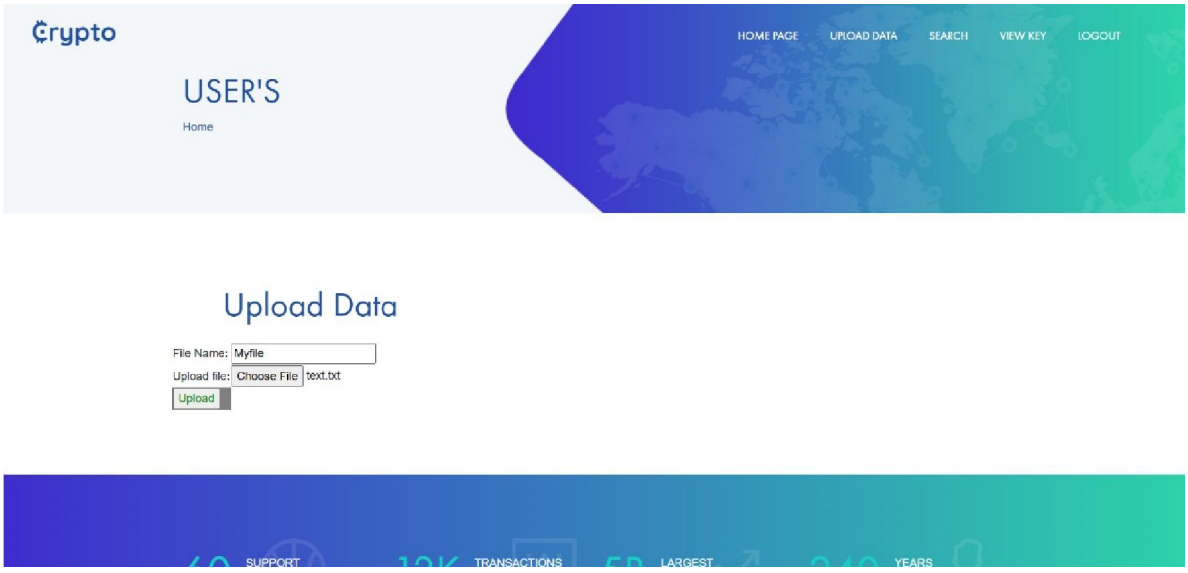
Upon executing the program and pasting the web address into the browser, the homepage is the initial loaded page. It serves as the primary point of interaction with the website or web application, indicating the initiation of browsing activities.

USER LOGIN PAGE



Following the click of the login button, the Login page becomes visible, prompting the entry of details. This sequence illustrates the transition from initiating the login process to providing necessary information for authentication. It underscores the procedural nature of user interaction in accessing secured areas of a website or application.

SIGN UPLOAD PAGE



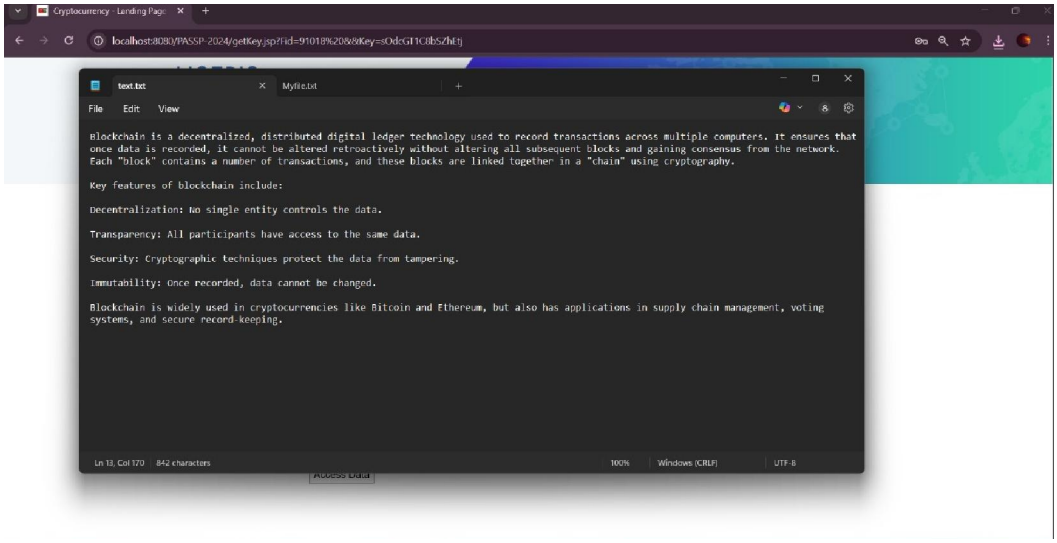
Upon successful login, a page allowing selection of the ASL image is presented. The user then chooses the desired image before submitting it. This process illustrates the post-login navigation flow, emphasizing user interaction in selecting and submitting the appropriate image for further action.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 5, Issue 6, June 2025
Impact Factor: 5.731

File Details

Fid	File Name	User Id	Key	Access
91018	Myfile	user2@gmail.com	sOdcGT1C8bSZhEtj	Download

FINAL RESULT PAGE



Following detection, the system provides the outcome along with the probability of accuracy. This step highlights the informative feedback loop, offering users insights into the reliability of the detection process.

VI. CONCLUSION

As the number of data abuse scandals involving service providers increases, so does the need to strengthen the protection of user data, for example by minimizing the risk of exposure to service providers during the authorization process. Therefore, we proposed a private authorization scheme-oriented service providers (PASSP) in Web 3.0 concept, which is the first private authorization scheme to minimize privacy risks associated with service providers. Specifically, the trustless authorization authentication method uses zero-knowledge proof technology as the core to hide the authorization relationship in authorization, and conducts public verification on the blockchain, so that the adversary cannot obtain any authorization object and content. The decentralized publicly verifiable proxy re-encryption method based on IPFS proposed in our scheme guarantees the security and integrity of the data during the authorization process and also prevents adversaries from profiting from it. Besides, we evaluated both the security and the performance of the

scheme to demonstrate its utility. For example, the on-chain verification time of zero-knowledge proof is generally less than 1.5s, and on the other hand, the re-encryption verification time is in milliseconds.

VII. FUTURE ENHANCEMENT

As a part of future work, we would like to extend our study toward continuous sign sentence recognition. We would also like to design a framework for handling the segmentation ambiguities and moment epenthesis in continuous sign language recognition. The isolated word gesture recognition framework could also be integrated to enhance sign spotting from continuous sign video stream for recognition sign sentences from continuous sign gestures. We also intend to increase the dataset and publicly publish it for further research.

REFERENCES

[1]. L. Mathews, "Equifax data breach impacts 143 million Americans." 2017. Accessed: Sep. 11, 2023. [Online]. Available: https://www. forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts143-million-americans

[2]. S. Gressin, "The Marriott data breach." 2018. Accessed: Dec. 20, 2023. [Online]. Available: https://consumer.ftc.gov/consumer-alerts/2018/12/ marriott-data-breach.

[3]. K. Conger, "Uber settles data breach investigation for $148 million." 2018. Accessed: Sep. 21, 2022. [Online]. Available: https://www. nytimes.com/2018/09/26/technology/uber-data-breach.html

[4]. D. Deahl, "Verizon partner data breach exposes millions of customer records." 2017. Accessed: Sep. 21, 2022. [Online].

[5]. M. Isaac and S. Frenkel, Facebook Security Breach Exposes Accounts of 50 Million Users, New York Times, New York, NY, USA, vol. 28, 2018, Accessed: May. 13, 2023. [Online]. Available: https://www. nytimes. com/2018/09/28/technology/facebook-hack-data-breach. html

[6]. C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., Bethesda, MD, USA, May 2009, pp. 169–178.

[7]. O. Goldreich, The Foundations of Cryptography—Volume 2: Basic Applications. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[8]. M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1. Helsinki, Finland, Aug. 2015, pp. 57–64.

[9]. S. Kim, K. Lee, W. Cho, Y. Nam, J. H. Cheon, and R. A. Rutenbar, "Hardware architecture of a number theoretic transform for a bootstrappable RNS-based homomorphic encryption scheme," in Proc. IEEE 28th Annu. Int. Symp. Field-Programmable Custom Comput. Mach., Fayetteville, AR, USA, May 2020, pp. 56–64.

[10]. J.E. Ekberg, K. Kostiainen, and N. Asokan, "The untapped potential of trusted execution environments on mobile devices," IEEE Security Privacy, vol. 12, no. 4, pp. 29–37, Jul./Aug. 2014.

[11]. G. Ayoade, V. Karande, L. Khan, and K. Hamlen, "Decentralized IoT data management using blockchain and trusted execution environment," in Proc. 19th IEEE Int. Conf. Inf. Reuse Integr., Salt Lake City, UT, USA, Jul. 2018, pp. 15–22.

[12]. D. G. Nair, V. P. Binu, and G. S. Kumar, "An improved E-voting scheme using secret sharing based secure multi-party computation," 2015, arXiv:1502.07469.

[13]. M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," in Proc. Int. Conf. Theory Appl. Crytograph. Techn., Bruges, Belgium, May 2000, pp. 539–556.

[14]. X. Fu, H. Wang, P. Shi, X. Ma, and X. Zhang, "Teegraph: Trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains," Sci. China Inf. Sci., vol. 65, no. 3, pp. 1–3, 2022.

[15]. J. De Clercq, "Single sign-on architectures," in Proc. Int. Conf. Infrastruct. Security, Bristol, U.K., Oct. 2002, pp. 40–58.

[16]. D. Hardt, "The OAuth 2.0 authorization framework," RFC 6749, IETF, pp. 1–76, 2012.