Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 4-B, pp. 1265–1279
DOI : 10.47974/JDMSC-2265

AI-generated privacy-preserving protocols for cross-cloud data sharing and collaboration

Asma Ibrahim Hussein *
Mohammed Ibraheem Hussein †
Ohood Saadoon Hlail §
Ministry of Higher Education and Scientific Research
Baghdad
Iraq

Abstract

With the rapid evolution of cloud computing, individuals and organizations are managing data storage and collaboration in an entirely new way. Using blockchain technology, this paper introduces CloudShare, a new framework for sharing and collaborating across clouds using a secure, decentralized ecosystem. As a result of the proposed system, storage costs and upload bandwidth requirements are significantly reduced while data confidentiality and consistency are maintained. With CloudShare, you can encrypt and deduplicate data without relying on centralized authorities to protect your privacy. Simulated results demonstrate that the model is capable of optimizing resource utilization and efficiently securing sensitive data. A decentralized architectural model overcomes the limitations of traditional centralized cloud models, opening the door to innovative cloud computing applications.

Subject Classification: *Primary 91G20, Secondary 01-08.*

Keywords: *AI-Generated, Cloud data, AI.*

1. Introduction

Organizations and individuals are increasingly turning to third-party cloud storage services to store their data. Cloud data volumes are proliferating, resulting in a dramatic increase in storage space and upload bandwidth demands [1]. For more than 50 years, Moore's law has powered

* *E-mail:* cs.20.10@grad.technology.edu.iq (Corresponding Author)
† *E-mail:* eng.mohammd.ibraheem@gmail.com
§ *E-mail:* Ohoodsaadoon146@gmail.com

the IT rebellion, but Waldrop [2] predicts it's coming to an end. CSPs are under increased pressure to maintain low costs in this environment.

The Sharing Economy [3] led us to imagine a scenario in which companies combined their cloud storage using blockchain technology to form a giant alliance cloud without a trusted centre authority [4]. Blockchain technology, combined with CSPs' ability to share a tamper-proof ledger, eliminates the need for third parties and possibly enables them to collaborate in new and unprecedented ways. By using this software, you can effectively integrate and allocate various cloud resources. Suppose each cloud serves its users; thus, CSP1's client, C1, might be interested in uploading a file to CSP2, but CSP2's client would upload it to its own cloud. Using blockchain, the CSP1 learns that there is another copy in CSP2 and records the ownership rather than storing the file itself. It doesn't matter whether the cloud stores all the files; it only needs to present them as such. C1's download of the file is implicitly done from CSP2's, so only a small fee needs to be paid to CSP2.

Our key contributions are summarized below:

- The purpose of our research is to examine how multiple clouds can work together in tandem to efficiently allocate resources without involving a third party, thereby reducing the gap between the speed at which data is generated and the speed at which it is stored, a benefit for organizations with limited storage resources at the moment. The scenario is then described in terms of its feasibility.
- Currently, no deduplication model allows multi-clouds to transparently deduplicate encrypted data between cross-users by using blockchains (ledgers) to record file existence and ownership. This deduplication scheme eliminates the need for separate servers, unlike other deduplication schemes. In addition to drastically reducing cloud storage costs, our scheme saves users' upload bandwidth while maintaining data confidentiality.
- Simulating CloudShare demonstrates its effectiveness and efficiency.

It is essential to our society that we communicate and collaborate [5]. As a result, Unified Communications and Collaboration (UCC) schemes have evolved due to technological advancements and changing communication needs. As collaboration systems undergo a dramatic shift to cloud-based deployments, security and privacy are not adequately addressed in UCC platforms [5]. A broader cross-section of the IT industry

has been adopting the cloud amid concerns surrounding regulated data, geopolitical constraints, and fundamental performance limitations. Even with a cloud-first approach, it is not possible to migrate all your data and use cases to the cloud or centralize your entire infrastructure. Several factors drive these use cases, including data sovereignty, low latency, portability, and bandwidth requirements. In IoT scenarios, a hybrid cloud/edge/fog computing paradigm has been tested to solve this problem [6].

The lack of a centralized architecture in the current public cloud era discourages the integration of collaboration edges and distributed ecosystems. Although cloud topologies have developed rapidly, distributed collaboration in multi-environment environments still faces a significant research gap [7]. An updated regulation was published in the Official Journal of the European Union on 14 September 2022 [8] that requires UCC service providers to ensure their interpersonal communications services are interoperable with those of other providers. Customers must be able to send and receive text messages end-to-end through separate platforms to utilize UCC services. As part of end-to-end communication, UCC providers must facilitate the exchange of images, voice messages, videos, and other documents.

An AIGC is a method for creating high-quality, personalized, and fast-paced content based on user input at a lower cost [9]artificial intelligence-generated content (AIGC, [10], [11]. With AIGC, instead of relying on UGC and PGC, large amounts of content can be produced cheaply and efficiently through automation [12]due to the instability of AIGC models, e.g., the stochastic nature of diffusion models, the quality and accuracy of the generated content can vary significantly. In wireless edge networks, the transmission of incorrectly generated content may unnecessarily consume network resources. Thus, a dynamic AIGC service provider (ASP. Various emerging applications, including metaverses and digital twins, would benefit from this technology [13] [14]. Users can play, collaborate, and socialize in a virtual world with AIGC, for example, in Roblox, with personalized skins and 3D game scenarios [15].

2. Related Work

As cloud computing has evolved since its inception, it has become increasingly sophisticated. There are numerous challenges associated with connecting to, accessing, maintaining, and securing data in the standard cloud computing model [16], which relies on a distant cloud data centre. Thousands of customers can be without critical services when

cloud services are unavailable due to failures in networks or data centres. As users generate and upload ever-increasing amounts of data, the cloud has become increasingly important in recent years.

Cloud computing is brought to users' doorsteps through this service. To accomplish this, routers, switches, base stations, etc., can be implemented with a limited amount of cloud-like functionality. Linked to their parent clouds, these mini-clouds provide prompt decision support using the data generated by users, for example, in autonomous vehicles or healthcare. After aggregating and analyzing the data, the edge network ultimately sends less data back to the core network for further analysis after the decision is made. Due to the lack of standardization, each implementation's features are classified differently [17]researchers in the field have already made the leap to envision Inter-Cloud computing. Their goal is to achieve better overall Quality of Service (QoS.

As a result of edge computing, IoT systems and smart devices become more responsive to decisions. The devices and infrastructure used for edge computing differ significantly in terms of functionality and power. Data storage and processing at the edge are limited due to the constraints of the edge computing model, such as the requirement for high-performance computing without real-time processing. A de-facto solution for enhancing the performance of traditional cloud computing for data of this type is to use multiple clouds as intercloud models. Here are a few seminal works that illustrate how multiple clouds can be effectively utilized [18], [19], [20], [21], [22]. Similarly, "cloud of clouds" and "cloud fusion" are terms that have been used in conjunction with intra-clouds [23]. Inter-cloud models are defined in the following manner [24].

In terms of cloud computing security, there are many surveys available. While some of them are relevant, they are outdated for a field with such rapid development. Others do not consider cloud computing's privacy [25]. Several existing surveys focus on specific applications and do not provide a roadmap for cloud computing in the future. To address these shortcomings, we have written this paper.

Using cloud computing as an example, the author discusses how privacy can be safeguarded in the cloud, and he offers some suggestions for future research [26]. Researchers reviewed articles regarding privacy and security in cloud architecture as well as encrypted and non-encrypted methods of securing electronic health records [27]. The vulnerability of cloud computing in terms of confidentiality, integrity, availability, accountability, and privacy preservation has been examined in [30], and strategies have been proposed to protect these vulnerabilities. A study

published in [31] aimed to find a method of improving privacy in cloud computing by analyzing privacy-enhancement technologies. In [28], we provide a review of techniques and patterns for protecting and encrypting data, as well as issues and approaches that can be explored in the future. Examining cloud computing [28] by examining its structure, concept, and adventures, as well as risks associated with security and privacy. The author of the article has presented several implementation techniques that can assist developers in the could-system environment, as well as privacy issues to consider in the environment [29]. In contrast to [29-31], instead of analyzing various cloud computing architectures in order to identify threats, the authors of this paper focused on security and privacy concerns. In addition, Bloom filtering is a method for encrypting data.

The majority of personal clouds allow users to interact with their cloud server directly by using a client. In addition, some clouds even allow partners to collaborate on file editing. Because of its simplicity, the collaboration functionality can be seen as a significant advance over static URLs and web access used by non-computer professionals. It even overwhelms widely used software like Git and SVN because it's so easy to use.

Our paper seeks to achieve sound user-perceived performance even under heavy, frequent file editing workloads, even when using inefficient web APIs. We were able to achieve this by observing two key things in real life. As a first step, we always have one or several nearby (client) proxies capable of efficiently accessing the web APIs of popular cloud storage services. The second problem is that there is substantial similarity between versions of files during file collaboration. By exploiting this, data sync time can be significantly reduced and interproxy traffic reduced.

3. Proposed Methodology

i. System Summary: System Model**.** Data collaboration across clouds can be secured by combining IBC and PRE techniques. This diagram illustrates the common system components of our scheme, including the trust authority, the data owner, the cloud provider, and the proxy server as shown in Figure 1.

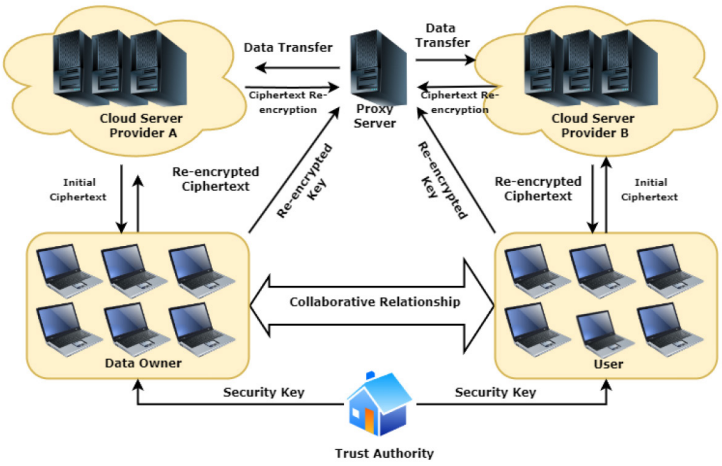

Figure 1

An overview of our system's system model.

- **Trust authority.** Trust authorities are trustworthy parties that generate initialization parameters for the system. Users' identities are also used to generate secret keys.
- **CSP.** In addition to providing data storage service, the CSP assists authorized users in accessing cipher texts that are stored on its servers.
- **Proxy server.** CSPs and proxy servers exchange data through web APIs. Furthermore, it can be used to generate re-encrypted cipher text, making it possible to collaborate across clouds.
- **Data owner.** CSPs receive ciphertext uploaded by data owners encrypted with IBE or IBBE algorithms. CSPs do not permit users to access data directly, so data owners must transmit re-encryption keys to proxies to allow encrypted cipher texts to be accessed.
- **User.** Using the user's secret key, the cloud-stored cipher text can be decrypted. Data is simultaneously decrypted by users with their secret keys and re-encrypted by the CSPs, resulting in data collaboration between the CSPs.

3.1.2 Security Requirements

Trust authorities are assumed to be trustworthy parties that will not collude with unauthorized parties. CSPs and proxy servers may collude,

however, to obtain unauthorized information if they are honest and curious. Here are the specific security requirements.

1. **Data confidentiality.** In addition to preventing unauthorized users from accessing the data, it should also prevent access by semi-trusted CSPs.
2. **Re-encryption secrecy**. The ciphertexts shouldn't be successfully transformed by someone who has access to a re-encryption key.

3.1.3 System Definitions

As part of our ACPRE protocol, we propose four different types of collaboration for cypher text.

Re-encryption of individual data between individuals, type I. Proxy servers encrypt the cypher text of one authorized user and re-encrypt it for the next authorized user.

Re-encryption of individual data between individuals, type II. In proxy servers, cypher texts for a group of users are re-encrypted based on the initial cipher text for one authorized user.

Re-encryption of individual data between individuals, type III. To create unique ciphertexts for each individual, proxy servers re-encrypt the ciphertext associated with the initial authorized user.

Re-encryption of individual data between individuals, type IV. With the help of a proxy server, the initial encryption of the cypher text for a set of users is re-encrypted according to their licenses.

Based on the above protocol, we implement it using the following algorithms.

1. **Setup (1^{λ}, *N*).** Based on the safety stricture γ and the maximum receiver set size N, the trust authority generates *PK* and *MK* for the system public key.
2. **KeyGen(PK, MK, ID).** Belief authorities receive inputs PK, MK, and IDs and output secret keys.
3. **IBE.Enc(PK, M, ID, C).** This process is based on inputs of PK, data M, identity ID, and condition C, which are then used to generate the initial ciphertext (CT_{IBE}.
4. **IBBE.Enc(PK, M, U, C).** With inputs of PK, M, U of identities, and C, the CSP produces an initial ciphertext. CT_{IBBE}.

An encrypting method of type I

5. **IBE.ReKeyGen1(PK, ID, SK, ID′, C).** An inputted *PK, SK,* user ID′, and condition *C* are combined to generate a re-encryption key.
6. **IBE.ReEnc1(PK, RK, CT_{IBE}).** The proxy server receives as inputs the *PK,* the re-encryption key *RK*, and the initial ciphertext CT_{IBE}. It outputs the re-encrypted ciphertext CT'_{IBE}.

An encrypting method of type II

7. **IBE. ReKeyGen2 (PK, ID, SK, U′, C)**. Users input *PK,* their identities *ID*, and secret keys SK, and then they output an encryption key *RK* based on the condition *C*.
8. **IBE.ReEnc2(PK, RK, CT_{IBE}).** An initial cypher text is an input to the proxy server, along with PK, RK, an encrypting key, and an encrypted text CT'_{IBBE} is output.

An encrypting method of type I

9. **IBBE.ReKeyGen1(PK, ID, SK, U, ID′, C).** Inputs in this process are *PK, SK,* the identity *ID* of the user, the *ID* of the authorized users, as well as a condition *C*. So, the user outputs a re-encryption key with RK as the result of these inputs.
10. **IBBE. ReEnc1(PK, ID, RK, U, CT_{IBBE}).** It receipts as effort the first ciphertext CT_{IBE}, the second ciphertext CT'_{IBE}, and the re-encryption key RK.

3.1.4 System Workflow

Figure 2 illustrates how the system workflow works. In the initialization phase of the system, the trust authority generates a public key and a master secret key by using the Setup algorithm. The KeyGen algorithm is used within the system to generate user secrets. Data owners run IBE at first. Either ENCI or IBBE. Data is encrypted with its identity and a keyword as conditions using the EC algorithm. There are ten data owners whose encrypted data is handled by CSPs. The user can obtain the ciphertext from the same CSP if the data owner has access to the same CSP. In response to the request for ciphertext, the CSP sends it to the user. There is a possibility that it runs IBE based on the intended user. Choosing between a Dec1 and an IBBE. The cryptographic ciphertext is decrypted

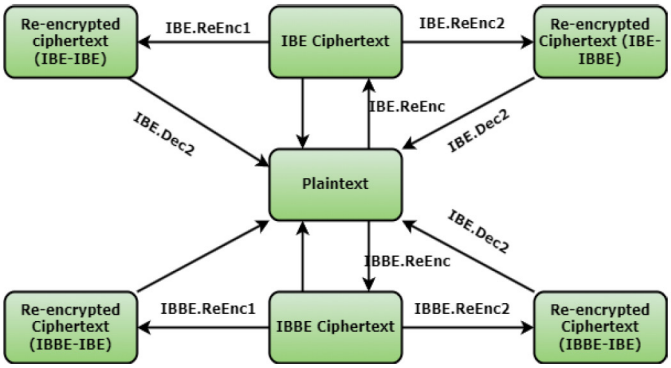

Figure 2

Our scheme's system workflow

using Dec1 using a secret key. A proxy server allows users to upload their re-encryption keys to re-encrypt data containing new identities and keyword conditions using re-encryption key generation algorithms. A new identity can be provided to a user, and they can access data by using the encryption key. Proxy servers re-encrypt ciphertexts using re-encryption algorithms. CSPs would re-encrypt ciphertexts when receiving access requests from users. Users can execute IBEs. Re-encrypted ciphertexts with Dec2 algorithm.

3.2 *Analyzing security risks*

3.2.1. Precision

A DK can be generated from a re-encrypted ciphertext CT' when the collaboration type supports it.

(1) As CT' is a re-encrypted ciphertext CT_{IBE} of Type I, it is computed as follows:

$$DK = C_1'.e(u^s, C_2') = DK - e(u^s, h^{-k})^{\gamma + H_1(ID)}.e(u^s, h^{k(y+H_1(ID))}) \quad (1)$$

(2) As CT' is a re-encrypted ciphertext CT_{IBE} of Type III, it is computed as follows

$$DK = C_1'.e((u^s, C_2') = DK - e(u^s, h^{-k})^{\prod_{ID_i \in U}\left(\frac{\gamma + H_1(ID_i)}{H_1(ID_i)}\right)}.e\left(u^s, h^{k\left(\prod_{ID_i \in U}\left(\frac{\gamma + H_1(ID_i)}{H_1(ID_i)}\right)\right)}\right) \quad (2)$$

(3) As CT' is a re-encrypted ciphertext CT_{IBE} of Type II, it is computed as follows

$$DK = C_1'.e((Z,C_3') = DK - e((ut^{\alpha})^{s},h^{-k})^{\prod_{ID_i \int U}\left(\frac{\gamma+H_1(ID_i)}{H_1(ID_i)}\right)}.e\left(h^{s},(ut^{\alpha})^{k\left(\prod_{ID_i \int U}\left(\frac{\gamma+H_1(ID_i)}{H_1(ID_i)}\right)\right)}\right) \tag{3}$$

Scheme Security. With DBDH, we are able to protect shared data against chosen plaintext attacks (CPAs). We are CPA-secure when adversary A and challenger C play against each other in a random oracle model.

Proof: There are U^* Challenges that adversary A chooses from. In challenger C, the Setup algorithm is used to create a PK and MK, and to generate H_1, H_2 and H_3 using three random oracles. It is also possible for an adversary to challenge challenger C by issuing queries for key generation or re-encryption key generation. A challenge message m_0 and m_1 is sent by the adversary to challenger C, which then generates a challenge ciphertext CT' by a random choice of b. In order to confirm challenge C, the challenge ciphertext is sent to the adversary A. During the guessing phase, the adversary guesses $b' \in \{0, 1\}$ are output. Our scheme will also be vulnerable to attack by adversary A, as it can defeat the CPA security of IBE and IBBE schemes and solve the DBDH problem in the re-encryption key generation process.

IBE or IBBE protects the random cryptographic key DK by encrypting the data with a symmetric key DK. In addition to symmetric encryption, the IBC scheme's security shields outsourced data against unnamed unauthorized users. User re-encryptions are not allowed without eligibility or ownership of the identity set. The DK cannot be determined from the ciphertext or re-encryption key.

4. Result and Discussion

An interconnected ecosystem relies on the establishment of trust relationships. It is proved that centralizing management ensures trust within these systems most effectively. As a result, sensitive data will be protected at a higher level than it was previously. The download time for the file, however, is directly proportional to the file size. In this system, files with larger sizes also take longer to download for multiple users (denoted as 'n' users). According to Figure 3, there is a relationship between these two variables.

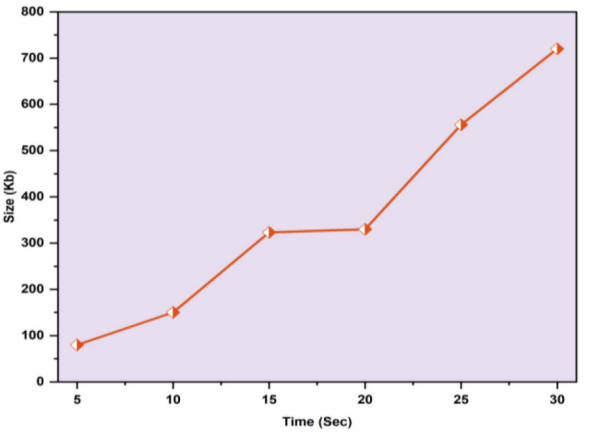

Figure 3

A cloud-based server's performance

As shown in Figure 4, CPU usage is reduced slightly when implementing a virtual network concept. Furthermore, each provider's time spent verifying the integrity of files is minimized, improving efficiency.

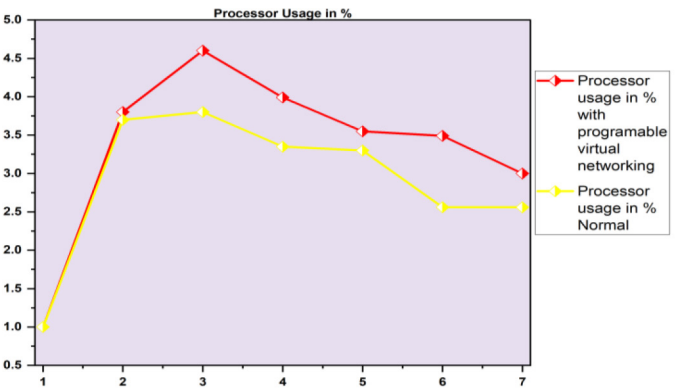

Figure 4

Utilization of processors

In this performance evaluation, the authentication server is evaluated for its ability to ensure that legitimate users are connected in a secure and filtered manner. It is analyzed how well the server manages security during active sessions by tracking the server's performance. Data and

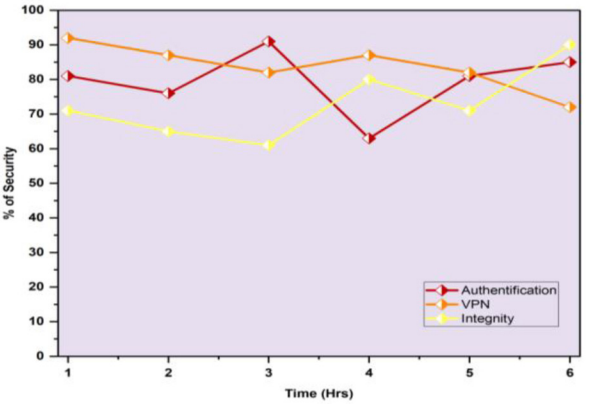

Figure 5

The system's performance

connections are protected from unauthorized access by filtering, while they are protected by security by allowing only authorized access. According to the findings, the server effectively maintains these aspects. Here is a summary of the observed results (Figure 5).

5. Conclusion

The purpose of this study is to describe CloudShare, an innovative framework for cross-cloud data collaboration designed to address challenges in traditional cloud architectures. With CloudShare, multiple cloud providers can share data transparently, securely, and efficiently without relying on centralized authorities. With the proposed system, data confidentiality is enhanced, storage costs are reduced, and response times are minimized, allowing it to serve the needs of a wide range of organizations. Its scalability and performance are validated through simulations, demonstrating its practicality. Optimising system workflows and expanding CloudShare's range of applications will be part of future research, contributing to the evolution of secure and distributed cloud computing.

References

[1] S. Sharma, "Expanded cloud plumes hiding Big Data ecosystem," *Future Gener. Comput. Syst.*, vol. 59, pp. 63–92 (2016).

[2] M. M. Waldrop, "More than moore," *Nature,* vol. 530, no. 7589, pp. 144–148 (2016).

[3] J. Hamari, M. Sjöklint, and A. Ukkonen, "The sharing economy: Why people participate in collaborative consumption," *J. Assoc. Inf. Sci. Technol.*, vol. 67, no. 9, pp. 2047–2059 (Sep. 2016), doi: 10.1002/asi.23552.

[4] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.,* vol. 14, no. 4, p. 352 (2018), doi: 10.1504/IJWGS.2018.095647.

[5] T. Reisinger, I. Wagner, and E. A. Boiten, "Security and Privacy in Unified Communication," *ACM Comput. Surv.*, vol. 55, no. 3, pp. 1–36 (Mar. 2023), doi: 10.1145/3498335.

[6] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE Access*, vol. 8, pp. 85714–85728 (2020).

[7] M. Weidner, M. Kleppmann, D. Hugenroth, and A. R. Beresford, "Key Agreement for Decentralized Secure Group Messaging with Strong Security Guarantees," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event Republic of Korea: ACM, pp. 2024–2045 (Nov. 2021). doi: 10.1145/3460120.3484542.

[8] M. Müller and M. C. Kettemann, "European Approaches to the Regulation of Digital Technologies," Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian Nida-Rümelin· Bashar Nuseibeh· Erich Prem·, p. 623 (2024).

[9] J. Wu, W. Gan, Z. Chen, S. Wan, and H. Lin, "AI-Generated Content (AIGC): A Survey," Mar. 26 (2023), arXiv: arXiv:2304.06632. Accessed: Oct. 19, 2024. [Online]. Available: http://arxiv.org/abs/2304.06632

[10] M. Xu et al., "Unleashing the power of edge-cloud generative ai in mobile networks: A survey of aigc services," IEEE Commun. Surv. Tutor., 2024, Accessed: Oct. 19 (2024). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10398474/

[11] Y. Cao et al., "A Comprehensive Survey of AI-Generated Content (AIGC): A History of Generative AI from GAN to ChatGPT," Mar. 07 (2023), arXiv: arXiv:2303.04226. Accessed: Oct. 19, 2024. [Online]. Available: http://arxiv.org/abs/2303.04226

[12] H. Du et al., "Enabling AI-Generated Content (AIGC) Services in Wireless Edge Networks," Jan. 09 (2023), arXiv: arXiv:2301.03220.

Accessed: Oct. 19 (2024). [Online]. Available: http://arxiv.org/abs/2301.03220

[13] Y. Wang et al., "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surv. Tutor.*, vol. 25, no. 1, pp. 319–352 (2022).

[14] Hussein, A.I.. Hybrid: (NH–DH) a New Hope and Diffie–Hellman for Transmission Data in Cloud Environment. In: Swaroop, A., Kansal, V., Fortino, G., Hassanien, A.E. (eds) Proceedings of Fourth Doctoral Symposium on Computational Intelligence . DoSCI 2023. Lecture Notes in Networks and Systems, vol 726. Springer, Singapore. https://doi.org/10.1007/978-981-99-3716-5_66.

[15] B. Nedić, "Gartner's top strategic technology trends," *Proc. Eng. Sci.*, vol. 1, no. 2, pp. 433–442 (2019).

[16] P. Mell, "The NIST Definition of Cloud Computing," NIST Spec. Publ., pp. 800–145 (2011).

[17] N. Grozev and R. Buyya, "Inter-Cloud architectures and application brokering: taxonomy and survey," *Softw. Pract. Exp.*, vol. 44, no. 3, pp. 369–390 (Mar. 2014), doi: 10.1002/spe.2168.

[18] D. Bernstein, E. Ludvigson, K. Sankar, S. Diamond, and M. Morrow, "Blueprint for the intercloud-protocols and formats for cloud computing interoperability," in 2009 fourth international conference on Internet and web applications and services, IEEE, 2009, pp. 328–336. Accessed: Oct. 20 (2024). [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5072540/

[19] R. Buyya, R. Ranjan, and R. N. Calheiros, "InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services," in Algorithms and Architectures for Parallel Processing, vol. 6081, C.-H. Hsu, L. T. Yang, J. H. Park, and S.-S. Yeo, Eds., in Lecture Notes in Computer Science, vol. 6081. , Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 13–31 (2010). doi: 10.1007/978-3-642-13119-6_2.

[20] K. Keahey, M. Tsugawa, A. Matsunaga, and J. Fortes, "Sky computing," *IEEE Internet Comput.*, vol. 13, no. 5, pp. 43–51 (2009).

[21] B. Rochwerger et al., "The reservoir model and architecture for open federated cloud computing," *IBM J. Res. Dev.*, vol. 53, no. 4, pp. 4–1 (2009).

[22] K. Kelly, "The Technium: A Cloudbook for the Cloud." Retrieved (2017).

[23] K. Fujitsū-KK, Fujitsu scientific & technical journal: FSTJ. na (1965).

[24] A. Algamdi, F. Coenen, and A. Lisitsa, "A trust evaluation method based on the distributed cloud trust protocol (CTP) and opinion sharing," *Provider*, vol. 5, no. 17, p. 18 (2017).

[25] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Health Inform.,* vol. 24, no. 8, pp. 2146–2156 (2020).

[26] P. J. Sun, "Privacy protection and data security in cloud computing: a survey, challenges, and solutions," *Ieee Access,* vol. 7, pp. 147420–147452 (2019).

[27] Fadhil, Fadhil Abbas, Hussien Alhilo, Abdul F. T. and Abdulhadi, Mohammed T.. "Enhancing data security using Laplacian of Gaussian and Chacha20 encryption algorithm" *Journal of Intelligent Systems*, vol. 33, no. 1 (2024), pp. 20240191. https://doi.org/10.1515/jisys-2024-0191

[28] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: A survey," *Ieee Access,* vol. 8, pp. 131723–131740 (2020).

[29] E. Kavakli, C. Kalloniatis, H. Mouratidis, and S. Gritzalis, "Privacy as an integral part of the implementation of cloud solutions," *Comput. J.,* vol. 58, no. 10, pp. 2213–2224 (2015).

[30] Azmi Shawkat Abdulbaqi, Israa Falih Muslim, Asraa A. Abd Al-Ameer, and Ahmed J. Obaid, "Healthcare surveillance based on cloud computing utilizing mobile devices," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 4, pp. 1189–1196 (2023), doi: 10.47974/JDMSC-1566.

[31] Zainab A. Jawad and Ahmed J. Obaid, "A systemic literature overview of Fake News Challenge (FNC-1) dataset and its use in fake news detection schemes," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 4, pp. 1197–1206 (2023), doi: 10.47974/JDMSC-1567.

Received February, 2025