AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

A BLOCKCHAIN-BASED DECENTRALIZED FRAMEWORK FOR CERTIFICATE AUTHENTICATION AND ISSUER TRUST

Madiha Sadaf[1], Afshan Fatima[2], Ruqiya Fatima[3]
[1]PG Scholar, Department of CS, Shadan Women's College of Engineering and Technology, Hyderabad, Madihasadaf0205@gmail.com
[2]Assoc Professor, Department of CSE, Shadan Women's College of Engineering and Technology Afshafatima0889@gmail.com
[3]Asst Professor, Department of CSE, Shadan Women's College of Engineering and Technology ruqiyafatima2716@gmail.com

ABSTRACT:
It is crucial to confirm the legitimacy of educational degree credentials, particularly when hiring new employees, since falsified paperwork can seriously disrupt operations and reduce productivity. Conventional verification techniques are susceptible to delays, mistakes, and data manipulation because they mostly rely on human procedures and centralized databases. A single, safe platform for smooth communication between issuers, holders, and verifiers is absent from these systems. This study suggests a decentralized, blockchain-based issuer validation and certificate verification solution to overcome these drawbacks. The approach ensures data immutability and tamper resistance by storing certificate hashes on the blockchain using Ethereum. Every participant in the network is represented as a peer node, including the issuer, holder, validator, and verifier. Even in cases when the certificate cannot be located, a hash-based search method drastically cuts down on certificate lookup time. According to experimental evaluation, the system provides quick, dependable verification and is economical in terms of gas use. The maintenance and validation of certificates is made safe, transparent, and effective by this integrated method.
KEYWORDS: Blockchain, Ethereum, search optimization, authentication, and certificate verification.

1. INTRODUCTION

In today's digital environment, managing certificates specially making sure they are tamper-resistant and intact—is crucial. Conventional public-key certificates kept in distributed databases provide a certain amount of security, but they are less suitable for guaranteeing the authenticity of certificates over time since they are susceptible to flaws like central points of failure. The majority of educational institutions encountered phishing assaults (60%) and account compromise (33%) in 2020, which was the highest outcome of all verticals examined when it came to cloud data. Academic diplomas provided by educational institutions are vulnerable to falsification as a result of these dangers. The average cost to a corporation of hiring a candidate with fraudulent qualifications is $15,000. Furthermore, there could be significant social harm: in addition to having a weakened sense of ethics, a fraudulent degree holder is unlikely to have the necessary knowledge in his profession (achieved through rigorous training and examination), making him a serious threat in some fields. Strict verification processes are the conventional line of defense against phony credentials. Even though it is still used, manual verification is an antiquated method that lags in the fast-paced digital world of today, raising the possibility of mistakes. Significant security flaws are revealed by these disruptions, which are made worse by laborious conventional techniques. Conventional approaches that rely on centralized authorities provide a single point of failure that is susceptible to cyberattacks. Significant operational inefficiencies can result from even brief outages or data loss in such systems, which can interfere with hiring and academic procedures. Furthermore, this vulnerability makes it possible for certificates to be falsified, eroding the fundamental confidence that these systems are meant to maintain. Although traditional distributed databases offer some decentralization, they still depend on centralized control for essential functions like updates, data backup, and access management. Vulnerabilities brought about by this centralized control include the possibility of single points of failure and vulnerability to manipulation. For example, unapproved changes or data breaches may happen if the central authority overseeing the database is compromised, eroding confidence in the system. Furthermore, because stakeholders cannot independently confirm the legitimacy of documents without depending on the central authority, traditional systems are inherently opaque. Blockchain, as another internet generation, has the potential to solve these issues. Blockchain is now widely used in a variety of industries, including supply chain, healthcare, transportation, agriculture, smart homes, and more, to guarantee the confidentiality and privacy of user data. Over the past few years, scholars have given blockchain technology a lot of attention. Blockchain technology is a perfect solution for certificate validation and authentication because of its distributed ledger and tamper-proof properties. To guarantee the integrity and dependability of transactions, users use blockchain technology to implement "smart contracts" through programs and algorithms. The credibility of certificates is undeniable once they are recorded on the blockchain, removing the chance of unauthorized changes. Additionally, blockchain eliminates the single point of failure that comes with conventional techniques. Blockchain allows peer-to-peer transfer of

digital assets without the need for middlemen, in contrast to conventional techniques. Because of its decentralized network, the integrity of the validation infrastructure cannot be jeopardized by a compromised node. In order to solve the issues of certificate forgery, ineffective verification, and mistrust of conventional credential management systems, this project offers a blockchain-based certificate authentication and issuer validation solution. The system securely stores and verifies digital certificates while guaranteeing transparency and tamper resistance by utilizing the decentralized and unchangeable characteristics of blockchain technology. The idea removes reliance on centralized authorities and permits safe, automated certificate issuance and verification across several institutions by integrating smart contracts on the Ethereum blockchain. A group of reliable organizations that serve as blockchain network validators is introduced by the suggested approach. By using a consensus-based voting system, these validators are in charge of authorizing new certificate-issuing organizations, guaranteeing that only authentic and validated organizations are able to issue genuine certificates. To protect data privacy, each certificate issued by a reliable organization is digitally signed and cryptographically hashed; only the hash is kept on the blockchain. This method prevents unauthorized alteration or replication of credentials while guaranteeing certificate integrity.The project uses a Bloom Filter-based hash mapping technique to optimize certificate search and verification time in order to improve system performance. This method greatly reduces needless blockchain queries by enabling the system to swiftly ascertain if a certificate is present or absent, particularly in situations when certificates are defective or nonexistent. By designating erroneous certificates as invalid and providing updated versions, the system also facilitates the rectification of flawed certificates without compromising blockchain immutability. All things considered, the project offers a safe, economical, scalable, and effective solution for issuer validation and real-time certificate authentication in academic and professional settings.

2. STIMULATING

The scope of this project covers the development of an integrated blockchain-based certificate authentication system applicable to academic, professional, and organizational credentials. A decentralized Ethereum blockchain network facilitates communication between the system's numerous stakeholders, including certificate issuers, validators, holders, and verifiers. Secure certificate issuance, issuer validation by consensus voting, certificate verification via public blockchain access, and effective search optimization using Bloom Filters are the main objectives of the project. It also supports correction of defective certificates without violating blockchain immutability by marking invalid certificates and issuing updated versions. The system is public and internationally accessible for verification purposes even while it protects data privacy by only storing hashed certificate data on-chain. The project is appropriate for practical implementation in recruitment, education, and credential verification ecosystems since it is scalable to big institutions and high-volume verification scenarios. However, it keeps the solution lightweight and economical by not attempting to store big certificate files on-chain or establish certificate ownership through NFTs.

3. OBJECTIVE

This project's main goal is to use blockchain technology to create and execute a decentralized certificate authentication and issuer trust architecture that will guarantee the safe, open, and impenetrable administration of digital certificates. By using a distributed blockchain network for certificate storage and validation, the system seeks to do away with reliance on centralized verification bodies. Using Ethereum-based smart contracts to create immutable certificate records—which guarantee that issued certificates cannot be altered, forged, or removed without permission—is one of the main goals. The initiative aims to provide a reliable environment where companies, organizations, and educational institutions may effectively confirm the legitimacy of certificates. By putting in place a decentralized voting system that enables approved institutions to approve and certify new certificate issuers before they are allowed to join in the system, another goal is to increase issuer confidence. The framework seeks to increase trust in digital certification procedures and stop dishonest organizations from giving phony credentials. By integrating Bloom Filters, which facilitate quick and effective certificate lookup processes, the project also aims to shorten the time needed for certificate verification. To minimize blockchain storage needs and transaction costs, hash-based optimization approaches will be utilized. The system seeks to preserve data integrity and privacy while offering safe certificate issuance, storage, distribution, and verification. Ensuring that certificate verification may be carried out in real time without necessitating direct communication with the issuing institution is another goal. In order to effectively manage a large number of certificates and institutions, the framework is built to support scalability. By documenting all certificate-related activities on a publicly auditable blockchain ledger, it also seeks to increase transparency. The initiative aims to reduce administrative costs and manual intervention by automating verification operations with smart contracts. Additionally, it seeks to offer government organizations, businesses, and educational institutions a dependable and affordable alternative. The project's ultimate goal is to build a decentralized, scalable, secure, and reliable digital certificate ecosystem that

boosts trust in issuer validation and certificate authentication across many domains.

3.1 What The Project Is About

Because existing certificate management systems are mostly centralized, manual, time-consuming, and susceptible to fabrication and tampering, certificate verification has become a crucial concern due to the rapid rise of digital education and online recruitment. Particularly in delicate fields, falsified or changed academic and professional credentials can result in significant financial losses, jeopardized organizational integrity, and societal risks. Current verification systems provide single points of failure that are vulnerable to cyberattacks, data manipulation, and outages since they mostly rely on centralized databases and trusted third parties. Furthermore, existing systems frequently simply evaluate the content of certificates rather than the legitimacy of the issuing institution in a cohesive way, leading to fragmented, ineffective, and untrustworthy authentication procedures. A secure, decentralized, tamper-proof, and effective system that can concurrently verify certificates and certify issuers on a single trusted platform is therefore desperately needed.

4. EXISTING SYSTEM:

- The majority of the present systems for confirming educational degree certificates are manual or semi-automated, depending on conventional techniques like direct contact with issuing institutions, email correspondence, or physical document verification.
- These techniques are laborious, ineffective, and prone to human error.
- Additionally, they frequently lack a centralized or uniform methodology, which leads to dispersed verification procedures among various companies and institutions.
- The records are frequently kept in centralized databases, which leaves them vulnerable to single points of failure, illegal changes, and data breaches.
- Institutions that lack a strong digital infrastructure are particularly susceptible to tampering and certificate forging

4.1 Existing System Disadvantages:

- Centralized digital records and paper-based records are easily manipulated or falsified.
- Verification frequently necessitates direct communication with institutions, which causes delays and inefficiencies.

4.2 THE PROPOSED SYSTEM

- This paper presents a blockchain-based system designed to verify the validity of institutions issuing certificates and to confirm the authenticity of those certificates.
- The front end, where users interact, and the back end, where the blockchain framework functions, are the two main parts of the system. Institutions serve as certificate issuers on the front end.
- By communicating with the blockchain network, these organizations ask for the validation of the certificates they issue.
- The blockchain and Bloom Filter components are located on the back end, which receives user input from the front end.
- A group of organizations that make up the blockchain network are in charge of verifying the certificate issuers. Votes on the issuer's validation are recorded and certificate data is stored by a smart contract that is implemented on the public blockchain.
- The system uploads the certificate data to the blockchain, where it is safely kept, after verifying the certificate issuer. After then, the Bloom Filter is modified to maximize search times while the certificate is being verified.

4.2.1 Proposed System Advantage

- Hash functions drastically cut down on search time by enabling quick lookup of certificate entries.
- Every transaction on the public blockchain is transparent and verifiable by any member of the network.

5.METHODOLOGIES

1. Design of User Interfaces

The user must enter their username and password in order to connect to the server. The user can log in to the server directly if they have previously left; otherwise, they must register their information, including their username, password, email address, city, and country. To manage upload and download rates, the database will create an account for every user. The user ID will be used as the name. To access a certain page, you typically need to log in. The query will be searched and displayed.

2. User

The system's role identification and user authentication are handled by the User module. The system ascertains the user's status as an Admin, Institute, Student, or Verifier after they log in. The user is taken to the relevant dashboard and features based on the designated role. This guarantees safe and regulated access to system resources. It serves as the point of entry for every user.

3. Certificate Issuance

Digital certificates are created and distributed to students via the Certificate Issuance module. To guarantee authenticity and integrity, a distinct hash value is produced during the creation of a certificate. The system safely stores both the certificate and its hash. The learner is then given access to the issued certificate. This module aids in preventing unwanted changes and certificate forgeries.

4. Blockchain Storage

In a decentralized ledger, the Blockchain Storage module keeps track of certificate transactions. For every certificate, it generates a ledger entry and uses a blockchain structure to connect it to earlier entries. Transaction details are unchangeable once they are stored. This guarantees the traceability, security, and transparency of certificate records. It offers a long-term, impenetrable storage system.

5. Receiver

The Validation module confirms the reliability of the system's participating institutions. After reviewing the institution's operations, validators vote according to predetermined criteria. The institution is recognized as trustworthy and given permission to issue certificates if validation is successful. The system updates the institution's status appropriately. The legitimacy of certificate issuers is preserved by this procedure.

6.Bloom Filter

For effective certificate lookup and verification, the Bloom Filter module is utilized. It uses several hash functions to map certificate hash values into a bit array. This makes it possible to quickly determine whether a certificate record might be present on the blockchain. It increases verification performance and drastically cuts down on search time. Before blockchain validation, the module serves as a quick pre-check.

6.TECHNIQUE ALGORITHM USED

6.1 Proposed Algorithm

Hash Function Mapping (e.g., SHA-256)

A cryptographic hash function called SHA-256 (Secure Hash Algorithm 256-bit) converts input data of any size into a fixed-length 256-bit hash value. The original message is first transformed into a binary representation using the method. After that, padding bits are used to make sure the message length meets the necessary processing requirements. The resulting data is split into 512-bit blocks after the original message length is added to the padded message. Eight preset 32-bit hash values are initialized by SHA-256 as the initial state. Each message block is divided into sixteen 32-bit words, which are then combined with bitwise and mathematical operations to create sixty-four words. The technique uses logical operations including XOR, AND, OR, and bit rotations to compress each block in sixty-four rounds. Temporary values are created during each cycle and coupled with message schedule values and specified constants. High sensitivity to changes in input is ensured by these actions, which constantly alter the internal hash state. The results are appended to the current hash values once every round for a block is finished. Until all of the input has been processed, this procedure is repeated for each message block. Ultimately, a distinct 256-bit hash digest is created by concatenating the eight modified hash values. SHA-256 is very useful for integrity checking since even a small change in the input data produces an entirely new output hash. It is computationally impossible to reconstruct the original message from the hash because it is a one-way function. SHA-256 is frequently used in blockchain systems, digital signatures, password storage, and data authentication applications because of its efficiency, security, and resistance to collisions.

6.2 EXISTING SYSTEM

- **Manual or Semi-Automated Matching**

A data comparison and verification method called manual or semi-automated matching is used to find matching records, entities, or credentials across several databases. To maintain uniformity, the procedure starts with gathering records from various sources and standardizing their formats. Names, IDs, email addresses, timestamps, and document information are among the pertinent attributes that are extracted for comparison. In manual matching, records are directly examined by an administrator or authorized user to ascertain whether they correspond to the same entity. Using pre-established rules, similarity metrics, or keyword matching strategies, the system first conducts preliminary comparisons in semi-automated matching. The system finds possible matches by calculating similarity scores between chosen attributes. Uncertain situations are marked for human inspection, whereas records that satisfy a predetermined confidence threshold are automatically recommended as matches. After reviewing the recommended pairs, the reviewer verifies, rejects, or changes the matching choices. During this phase, discrepancies can be fixed and duplicate records can be combined. To increase accuracy, the procedure could additionally include validation against outside databases or reference materials. The records are linked or mapped within the system after matching decisions are made. To monitor verification activities and guarantee accountability, audit logs are kept up to date. By fusing human judgment with automatic efficiency, the method lowers errors. It is especially helpful when datasets have inconsistent, unclear, or incomplete data. When accuracy and dependability are crucial, manual or semi-automated matching is frequently used in blockchain-based validation systems, customer data integration, healthcare records management, identity management, and credential verification.

7. SYSTEM ARCHITECTURE

End Users, Application Software, Blockchain Network, and Certificate Verification Services are the four main parts of the system design. Digital certificates are uploaded and managed by educational institutions using the application software. A smart contract that is implemented on the public blockchain receives the certificate information from the institution when a fresh certificate is issued. Before the certificate is officially registered, it is validated and approved by a group of recognized institutions by voting. The certificate data is kept on

the blockchain after approval, guaranteeing transparency and immutability. Fast certificate lookup and verification are made possible by a Bloom Filter, which is updated and maintained each time a new certificate is added. Verification requests are submitted via the application software by clients or verifiers.

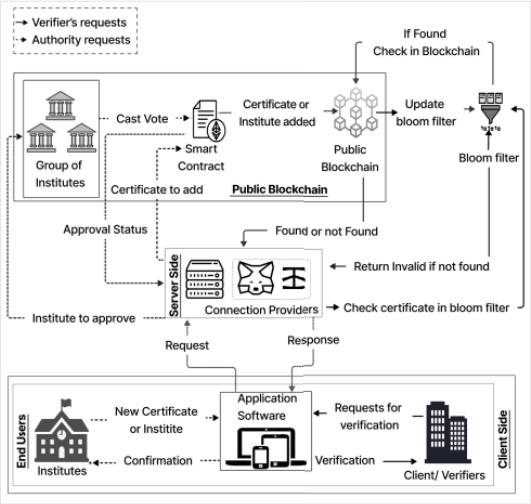
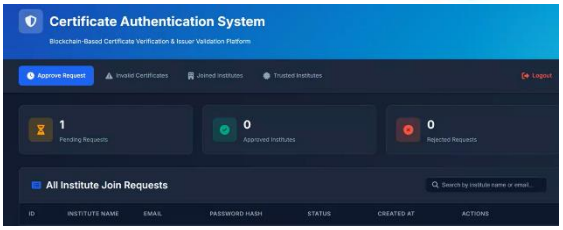
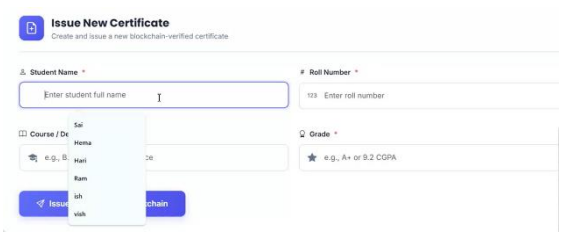


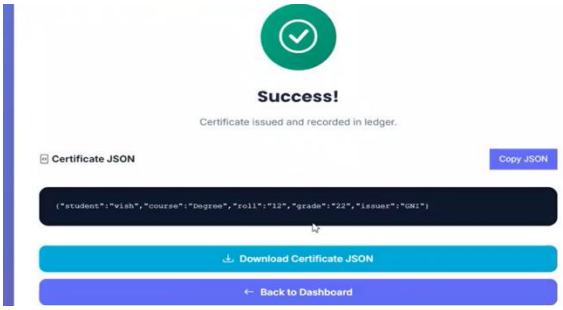
FIG:7 System Architecture

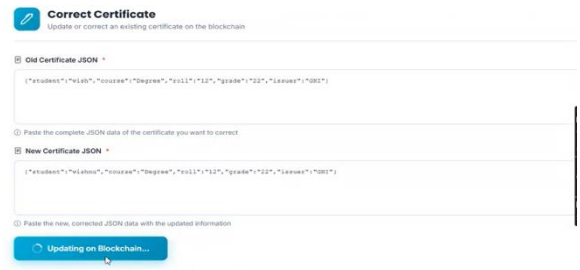
To swiftly ascertain whether the certificate might exist, the system initially examines the Bloom Filter. If the certificate is located, blockchain records are used for thorough verification. The request is deemed invalid and a suitable response is sent back if it cannot be located. Communication between individuals, organizations, and blockchain services is made easier by connection providers. Without the need for a centralized authority, smart contracts automate the processes of certificate registration, validation, and approval. Using blockchain technology, the architecture guarantees safe certificate storage, decentralized trust management, quick verification, fraud prevention, and transparent certificate authentication.

8. RESULT









9. CONCLUSION

The suggested blockchain-based certificate verification system offers a safe, open, and effective way to verify institutions and authenticate certificates. The solution prevents fraudulent actions by ensuring that only approved organizations can issue certificates through the integration of smart contracts with a public blockchain. Document authenticity and integrity are ensured by the immutability and tamper-proof nature of certificate data once it is recorded on the blockchain. While the incorporation of a Bloom

Filter greatly increases search speed during the verification process, the application of cryptographic hash algorithms improves data security. By removing reliance on a single authority, the decentralized validation mechanism fosters participant confidence. All things considered, the system provides a scalable and dependable framework for managing digital certificates, guaranteeing improved data safety, speedier verification, and transparency.

9.2 FUTURE ENHANCEMENT

Future improvements have the potential to greatly increase the decentralized certificate authentication and issuer trust system's efficacy, scalability, and uptake. The system can automatically identify fraudulent activity, detect unusual certificate issuing behavior, and anticipate possible security problems before they materialize thanks to the integration of artificial intelligence and machine learning algorithms. While preserving security, putting in place a multi-chain or hybrid blockchain architecture can increase transaction throughput, lessen network congestion, and save operating expenses. The system can be extended to facilitate cross-border certificate verification, enabling seamless credential verification for government agencies, employers, and educational institutions around the globe. Integration with Decentralized Identity (DID) frameworks can improve privacy protection and provide users more control over their personal data. Using smartphones and tablets, mobile application development can increase user access to certificate issuance, storage, and verification. By providing rapid and safe access to certificate information, QR-code-based instant verification helps streamline the validation process. To confirm the legitimacy of a certificate without disclosing private information, sophisticated cryptographic methods like Zero-Knowledge Proofs (ZKP) can be used. With little human involvement, smart contract automation can be improved to enable certificate renewal, revocation, and expiration management. Integration of cloud and edge computing can lower verification latency and enhance system performance. Practical adoption can be boosted by interoperability with digital learning platforms and current school administration systems. Users can learn about security events, verification requests, and certificate modifications using real-time notification systems. Support for professional licenses, digital badges, and skill certificates can also increase the system's usability in a variety of industries, resulting in an extensive and internationally recognized credential verification ecosystem.

REFERENCES

[1] A. Osseiran et al., “The foundation of the mobile and wireless communi cations system for 2020 and beyond: Challenges, enablers and technology solutions,” in Proc. IEEE Veh. Technol. Conf., 2013, pp. 1–5.

[2]Z.Xuetal.,“Age-aware data selection and aggregator placement fortimely federated continual learning in mobile edge computing,” IEEE Trans. Comput., vol. 73, no. 2, pp. 466–480, Feb. 2024.

[3] R. Bhardwaj et al., “Ekya: Continuous learning of video analytics models on edge compute servers,” in Proc. 19th USENIX Symp. Netw. Syst. Des. Implementation, 2022, pp. 119–135.

[4] X. Hou and S. Dey, “Motion prediction and pre-rendering at the edge to enable ultra-low latency mobile 6DoF experiences,” IEEE Open J. Commun. Soc., vol. 1, pp. 1674–1690, 2020.

[5] F. Nawab, D.Agrawal, and A. El Abbadi, “DPaxos: Managing data closer to users for low-latency and mobile applications,” in Proc. Int. Conf. Manage. Data, 2018, pp. 1221–1236.

[6] Amazon, “AWS wavelength for media & entertainment,” 2021. [On line].

[7] Z. Xu, Y. Fu, Q. Xia, and H. Li, “Enabling age-aware Big Data analytics in serverless edge clouds,” in Proc. IEEE Conf. Comput. Commun., 2023, pp. 1–10.

[8] E. Schurman and J. Brutlag, “The user and business impact of server delays, additional bytes, and HTTP chunking in web search,” Velocity Web Perform. Operations Conf., Oreilly, 2009.

[9] S.-C. Lin et al., “The architectural implications of autonomous driving: Constraints and acceleration,” in Proc. 23rd Int. Conf. Architectural Sup port Program. Lang. Operating Syst., 2018, pp. 751–766.

[10] S. Ma, S. Guo, K. Wang, W. Jia, and M. Guo, “A cyclic game for service-orientedresourceallocationinedgecomputing,”IEEETrans.Serv. Comput., vol. 13, no. 4, pp. 723–734, Jul./Aug. 2020.

[11] Z. Xu et al., “Collaborate or separate? distributed service caching in mobile edge clouds,” in Proc. IEEE Conf. Comput. Commun., 2020, pp. 2066–2075.

[12] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A survey on mobile edge computing: The communication perspective,” IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, Fourth Quarter 2017.

[13] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin, “Online collaborative data caching in edge computing,” IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 2, pp. 281–294, Feb. 2021.

[14] J. Zhou, F. Chen, Q. He, X. Xia, R. Wang, and Y. Xiang, “Data caching optimization with fairness in mobile edge computing,” IEEE Trans. Serv. Comput., vol. 16, no. 3, pp. 1750–1762, May/Jun. 2023.

[15] R. Luo, H. Jin, Q. He, S. Wu, and X. Xia, “Enabling balanced data deduplication in mobile edge computing,” IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 5, pp. 1420–1431, May 2023.

[16] X. Xiaetal., “Formulating cost-effective data distribution strategies online for edge cache systems,”

IEEE Trans. Parallel Distrib. Syst., vol. 33, no.12, pp. 4270–4281, Dec. 2022.
[17] E. Li, L. Zeng, Z. Zhou, and X. Chen, "Edge AI: On-demand accelerating deep neural network inference via edge computing," IEEE Trans. Wireless Commun., vol. 19, no. 1, pp. 447–457, Jan. 2020.
[18] B. Lietal., "Cooperative assurance of cache data integrity for mobile edge computing," IEEE Trans. Inf. Forensics Secur., vol. 16, pp. 4648–4662, 2021.
[19] J. Xu, L. Chen, and P. Zhou, "Joint service caching and task offloading for mobile edge computing in dense networks," in Proc. IEEE Conf. Comput. Commun., 2018, pp. 207–215.
[20] J. Peng et al., "MagNet: Cooperative edge caching by automatic content congregating," in Proc. ACM Web Conf., 2022, pp. 3280–3288.
[21] B. Li, Q. He, F. Chen, L. Lyu, A. Bouguettaya, and Y. Yang, "EdgeDis: Enablingfast, economical,andreliabledatadisseminationformobileedge computing," IEEE Trans. Serv. Comput., vol. 17, no. 4, pp. 1504–1518, Jul./Aug. 2024.
[22] Q.Xia, Z. Xu, W.Liang, S. Yu, S. Guo, and A. Y. Zomaya, "Efficient data placement and replication for QoS-aware approximate query evaluation of Big Data analytics," IEEE Trans. Parallel Distrib. Syst., vol. 30, no. 12, pp. 2677–2691, Dec. 2019.
[23] Amazon, "AWS DataSync," 2018, Accessed: Mar. 20, 2022. [Online].
[24] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin, "Cost effective app data distribution in edge computing," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 1, pp. 31–44, Jan. 2021.\
[25] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2508–2530, Jun. 2006.
[26] L.Yuanetal., "CoopEdge:Adecentralized blockchain-based platform for cooperative edge computing," in Proc. Web Conf., 2021, pp. 2245–2257.
[27] B. Li, Q. He, F. Chen, H. Jin, Y. Xiang, and Y. Yang, "Auditing cache data integrity in the edge computing environment," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 5, pp. 1210–1223, May 2021.
[28] B.Li, Q. He, L.Yuan, F. Chen, L. Lyu, and Y. Yang, "EdgeWatch: Collab orative investigation of data integrity at the edge based on blockchain," in Proc. 28th ACM SIGKDD Int. Conf. Knowl. Discov. Data Mining, 2022, pp. 3208–3218.
[29] Q. He et al., "A game-theoretical approach for mitigating edge DDoS attack," IEEETrans.DependableSecureComput.,vol.19,no.4,pp.2333 2348, Jul./Aug. 2022.
[30] C. Huang et al., "Erasure coding in windows azure storage," in Proc. USENIX Annu. Tech. Conf., 2012, pp. 15–26.
[31] K. V. Rashmi, N. B. Shah, D. Gu, H. Kuang, D. Borthakur, and K. Ram chandran, "A hitchhiker's guide to fast and efficient data reconstruction in erasure-coded data centers," in Proc. ACM SIGCOMM Conf., 2014, pp. 331–342.
[32] J.Yang,A.Sabnis,D.S.Berger,K.Rashmi,andR.K.Sitaraman,"C2DN: How to harness erasure codes at the edge for efficient content delivery," in Proc. 19th USENIX Symp. Netw. Syst. Des. Implementation, 2022, pp. 1159–1177.
[33] H. Jin, R. Luo, Q. He, S. Wu, Z. Zeng, and X. Xia, "Cost-effective data placement in edge storage systems with erasure code," IEEE Trans. Serv. Comput., vol. 16, no. 2, pp. 1039–1050, Mar./Apr. 2023.
[34] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in Proc. USENIX Annu. Tech. Conf., 2014, pp. 305–319.
[35] Y. Sahni, J. Cao, L. Yang, and Y. Ji, "Multi-hop multi-task partial compu tation offloading in collaborative edge computing," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 5, pp. 1133–1145, May 2021.
[36] L. He, F. Li, H. Xu, W. Xia, X. Zhang, and X. Tao, "Blockchain-based vehicularedgecomputingnetworks:Thecommunicationperspective,"Sci. China Inf. Sci., vol. 66, no. 7, 2023, Art. no. 172301.
[37] S. Li and T. Lan, "Hotdedup: Managing hot data storage at network edge through optimal distributed deduplication," in Proc. Conf. Comput. Commun., 2020, pp. 247–256.
[38] X. Xia et al., "Data, user and power allocations for caching in multi access edge computing," IEEETrans. Parallel Distrib. Syst., vol. 33, no. 5, pp. 1144–1155, May 2022.
[39] X. Xia et al., "Budgeted data caching based on k-median in mobile edge computing," in Proc. 27th IEEE Int. Conf. Web Serv., 2020, pp. 197–206.
[40] T. X. Tran and D. Pompili, "Adaptive bitrate video caching and process ing in mobile-edge computing networks," IEEE Trans. Mobile Comput., vol. 18, no. 9, pp. 1965–1978, Sep. 2019.
[41] T. Zhao, I.-H. Hou, S. Wang, and K. Chan, "Red/LeD: An asymptotically optimal and scalable online algorithm for service caching at the edge," IEEE J. Sel. Areas Commun., vol. 36, no. 8, pp. 1857–1870, Aug. 2018.
[42] P. Yang, N. Zhang, S. Zhang, L. Yu, J. Zhang, and X. S. Shen, "Content popularity prediction towards location-aware mobile edge caching," IEEE Trans. Multimedia, vol. 21, no. 4, pp. 915–929, Apr. 2019.
[43] Y. Jiang, M. Ma, M. Bennis, F.-C. Zheng, and X. You, "User preference learning-based edge caching for fog radio access network," IEEE Trans. Commun., vol. 67, no. 2, pp. 1268–1283, Feb. 2019.
[44]X.Ma,S.Wang,S.Zhang,P.Yang,C.Lin,andX.S.Shen,"Cost-efficient resource provisioning for dynamic requests in cloud assisted mobile edge computing," IEEETrans.CloudComput.,vol.9,no.3,pp.968–980,Third Quarter 2021.

[45] S. M. Azimi, O. Simeone, A. Sengupta, and R. Tandon, "Online edge caching and wireless delivery in fog-aided networks with dynamic content popularity," IEEE J. Sel. Areas Commun., vol. 36, no. 6, pp. 1189–1202, Jun. 2018.
[46] J. Gao, S. Zhang, L. Zhao, and X. S. Shen, "The design of dynamic probabilistic caching with time-varying content popularity," IEEE Trans. Mobile Comput., vol. 20, no. 4, pp. 1672–1684, Apr. 2021.