SSO-IDENTITY ACCESS MANAGEMENT SYSTEM FOR CLOUD APPLICATIONS

Umaima Siddiqua[1], Dr. Maniza Hijab[2], Dr. Fahmina Taranum[3]
[1]PG Scholar, Department of CSED, Muffakham Jah College of Engineering And Technology,
umaimasiddiquaaa@gmail.com
[2]Associate Professor, Department of CSED, Muffakham Jah College of Engineering And Technology,
manizahijab@mjcollege.ac.in
[3]Associate Professor, Department of CSED, Muffakham Jah College of Engineering And Technology,
ftaranum@gmail.com

ABSTRACT

Existing Single Sign-On (SSO) access control systems typically depend on standard frameworks that require additional authentication components and identity providers. With the increasing demand for outsourcing system resources, such as data and applications, to the cloud platform, conventional SSO models face challenges in enabling efficient and fine-grained access control for multi-user and multi-application environments. In this paper, we propose D2-IAM, a blockchain-based Identity and Access Management (IAM) system designed to enhance security for SSO in cloud environments, At its core, D2-IAM leverages blockchain and smart contracts to ensure robust and tamper-resistant access control. Our system Utilizes a hashed-based token mechanism for authentication, reducing the dependency on third-party identity providers and minimizing communication overhead. Furthermore, D2-IAM implements fine-grained access policies stored in a Blochian-backed database, enabling dynamic access control. Experimental evaluations conducted on Google Cloud demonstrate the efficiency of D2-IAM, achieving authentication and authorization performance up to three times faster than conventional methods.

1. INTRODUCTION

Access Control structure is overall seen as the most head and basic instrument of any information systems. An effective access control typically implies the safeguarded plan of 3As including affirmation, endorsement, and assessing. In dispersed registering, most expert associations give fundamental confirmation like client/secret expression, onetime mystery word (OTP) to their clients. Such confirmation parts may not be sufficient for ensuring the strong permission to essential or sensitive resources, for instance, applications or informational index arranged in the cloud. Most affiliations conveying their applications or any organizations on the cloud need to complete their entry control part, for instance, complex affirmation, PKI approval alongside their endorsement model on top of the organizations sent. For those affiliations having various application organizations on cloud could have different access control parts to different get-togethers of clients. The cost for dealing with confirmation decisions, access control approaches are luxurious. Possible some cloud providers could offer Single hint on affirmation structure to help endeavors having different systems. SSO engages a client to use a lone game plan of login certificates, for instance, character credits, client/secret word, two-factor check (2FA) or diverse affirmation (MFA) to get adequately near different systems. It will in general be executed by using security statement markup language (SAML) standard, token-based, confirmation standards. Lately, SSO applications impact OpenID Connection point and FIDO to engage more versatile and secure component of the affirmation cooperation. OpenID Point of interaction has been made as the person layer over OAuth 2.0 show which grants various types of clients, for instance, electronic applications, compact applications, and JavaScript clients, to affirm the character and help the profile of the end-client through the endorsement server. Also, The FIDO Alliance shipped off FIDO2 Affirmation standard considering public key cryptography for approval. It is recognized as another password less affirmation standard. For the check, clients can join up and subsequently select a FIDO2 security key upon the sign-in interface as their affirmation method. This procedure is a more secure approval that gives secure and fast login experiences across locales and applications. In any case, the SSO affirmation organization goes with additional help cost charged the resource owners can use the default approval strategy given by the cloud provider. In like manner, including different affirmation standards for SSO organization could deal with the clients' structure similitude, for instance, programs, run-time organizations. As to get to methodology the board, they need to migrate and execute separate endorsement plans for limiting the entry distinction to their clients in getting to different resources. Here, the investigating is achieved through the application log records and access logs maintained by the cloud provider. Regardless, using the check organization given by the providers could convey security and insurance issue. This is in light of the fact that the character information may be spilled or compromised. Additionally, dealing with various entry systems game plan for different resources in cloud isn't useful essentially. The organization cost is high in such environment. Also, SSO organization that relies upon gathered approval in the close by have server or in the cloud regularly encounters the failure point and it impels huge impact on the clients and business. Lately,

blockchain development has been taken on by a couple of assessment works focusing in on IAM [and data sharing. Various ventures will frequently take on blockchain for supporting their arrangement dealing with and sharing as it maintains decentralized, conspicuous, and tamper resistant data access control designing. These properties are needed for serving flexibility and dynamic control of different resources giving to minimization of point of failure of structure substances conveyed in cloud environment. Additionally, the components of IAM can be actually carried out by the execution of keen agreements. In spite of the way that blockchain development draws in the entry control the board areas of strength for with confirmation, high openness of organization and constant access trade conspicuousness, there is no specific solution for consolidate the decentralization model of blockchain advancement and a cloud-based permission control system having the properties of lightweight SSO approval, different access endorsement models with the security saving technique, and the execution of preventive-based permission control.

2. RELATED WORK

Most exploration works connected with a cloud-put together or circulated IAM centers with respect to the particular model, for example, job based [9], strategy-based admittance control, IAM principles and SSO Administration. The confirmation administration, for example, OpenID interface and FIDO2 have been utilized as the SSO highlight in numerous applications. OpenID associate is based on OAuth 2.0 convention that permits clients to utilize SSO to access across applications utilizing OpenID Suppliers (Operations) to validate their personalities. Notwithstanding, it needs client approval information like the honor or consent information. FIDO eliminates supplant the secret word verification with the PKI validation strategy in view of the key created upon sign-in or the critical put away in the gadget. This empowers both secure and quick login to a few applications. To manage this confirmation technique, clients need to go through an extra security step and need to mindful of the security of the critical put away in their gadgets. In, Moghaddam et al. proposed a strategy-based validation model to control client confirmation through the cosmology construction. The approval is done by means of access strategies put away in the arrangement data set. In any case, the paper doesn't manage different assets conveyed in the cloud framework.

3. METHODOLOGIES

D 2 - IAM System Model contains the going with substances and utilitarian structures. • Resource owner circulates or gives resources, for instance, application organizations on a public cloud and allows supported clients to get to. • Clients are allowed to get to different application organizations upon the entry game plans coordinated by the resource owner. • Access Control Organization Entryway (ACSG) is the middle structure organization arranged in the cloud. It is responsible for enduring access requests from the clients and liaising with the smart arrangements for performing SSO approval, token repudiation, executing endorsement, and gathering preventive access control. The doorway similarly controls the clients' entry meeting while they use the applications. All associated induction decisions are maintained through the ACSG.

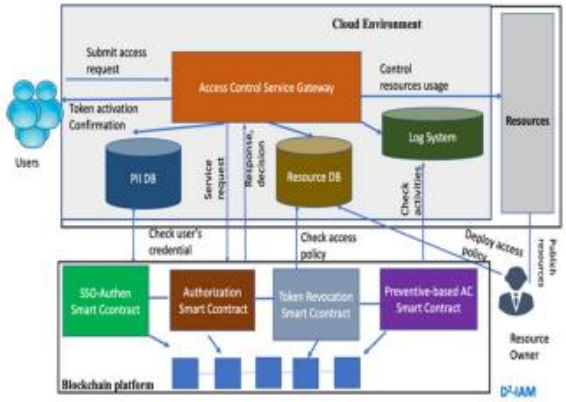


Fig 1. System Architecture

Splendid arrangements (SCs) are a lot of executable ventures running on the blockchain to execute the tasks considering reasonable capacity. Blockchain ensures that all canny arrangements are extremely durable and trades executed are freely and really executed with full obviousness. All began trades are timestamped and scattered across various center points in the association. This prevents ridiculing or change attack of the substance or the norm of the understanding. Also, astute arrangements don't require concentrated position to affirm their believability. Rather, they license individuals to do explicit trades in a speedier manner. To adjust to other security attacks, there are works that proposed the methodologies to give the defensive game plans like static examination, runtime ID, and language-based security. In our structure, we control the permission to clever arrangements considering the hash worth of system character code and address, for instance, IP or Mac address of the system modules set aside in the sagacious agreement. Expecting that the visitor's information fails to match the ones set aside in the arrangement amassing, the requesting for executing the understanding is dropped.

4. PROPOSED ALGORITHM

SINGLE SIGN-ON AUTHENTICATION SYSTEM

Existing SSO verification conspires for the most part depend on the conventional validation strategies, for example, SAML, OAuth which don't take the confirmation choices of numerous assets into their model. In the event that the confirmation administration or any believed substance who gives the personality or access ticket is compromised, the entire access control is breakdown.

MULTI-SYSTEM AUTHENTICATION

We contrived a lightweight SSO-confirmation token in view of most noteworthy validation level of the assets mentioned to get to. The verification is in this manner bound to the honour of asset access as opposed to depending on extra confirmation component. Our proposed SSO-verification token essentially decreases the correspondence above for multi-framework confirmation.

NON-BLOCKCHAIN ACCESS CONTROL SCHEMES

Most assessment works associated with a cloud-set up or coursed IAM focuses regarding the specific model, for instance, work based, methodology-based permission control, IAM standards, and SSO Organization. The check organization, for instance, OpenID interface and FIDO2 have been used as the SSO feature in various applications. OpenID partner depends on OAuth 2.0 show that grants clients to use SSO to access across applications using OpenID Providers (Activities) to approve their characters. Regardless, it needs client endorsement data like the honor or approval data. FIDO kills supersede the mystery expression affirmation with the PKI approval procedure considering the key made upon sign-in or the basic set aside in the device. This enables both secure and speedy login to a couple of utilizations. To deal with this affirmation technique, clients need to go through an additional security step and need to aware of the security of the essential set aside in their contraptions. In, Moghaddam et al. proposed a procedure-based approval model to control client check through the mysticism design. The endorsement is finished through move to courses of action set aside in the methodology informational collection. Nevertheless, the paper doesn't oversee different resources conveyed in the cloud structure.

BLOCKCHAIN-BASED PERMISSION CONTROL SCHEMES

Lately, numerous investigation works have used blockchain development as a phase to assist decentralized character the chiefs as well as the entry with controlling for data participating in circulated processing. For example, Wang et al. proposed a cloud client character the board show considering Ethereum blockchain. The character the chiefs is compelled by using insightful arrangements. This enables decentralized induction control and avoid the intercession by the cloud provider. It moreover engages clients and cloud providers to commonly manage the system through splendid arrangements. In any case, the proposed structure doesn't deal with the endorsement the leaders in the cloud setting.

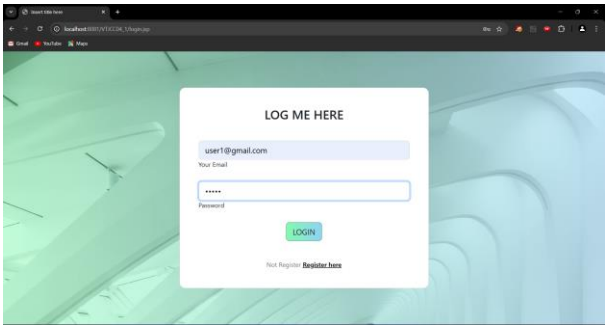


Fig 2. Admin Login Page

Fig 3. Admin Home Page

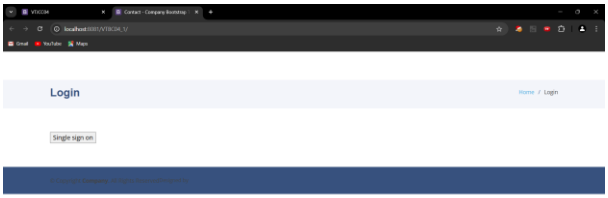


Fig. 4: Single Sign-On Page

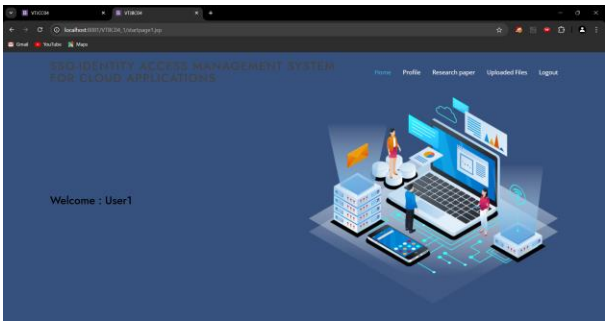


Fig 5. Single Sign-On Success Page

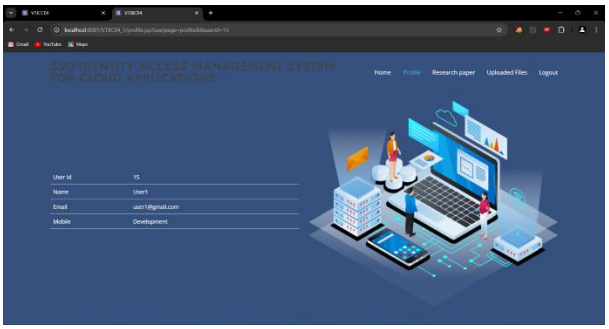


Fig 6. User Profile Page

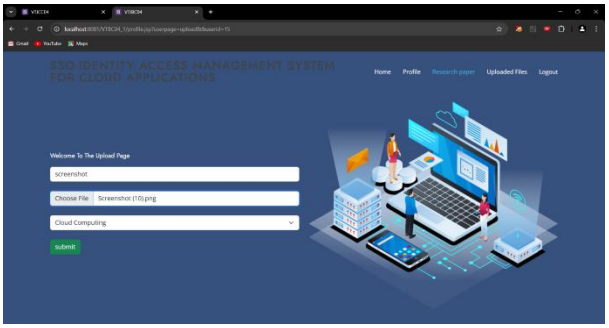


Fig 7. Upload Document Page

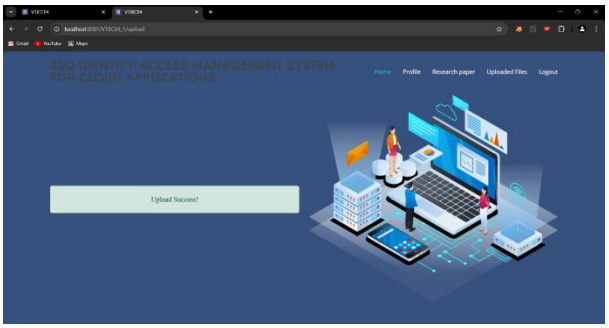
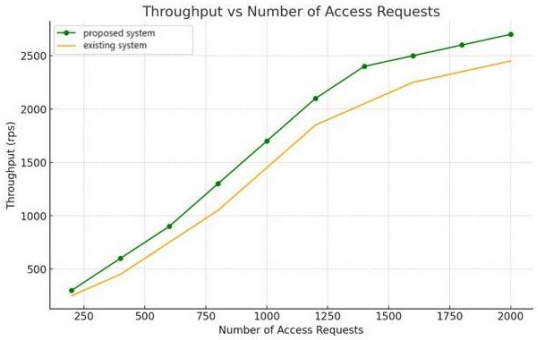


Fig 8. Document Upload Success

5. RESULT DISCUSSION

The graph titled **"Throughput vs Number of Access Requests"** compares the performance of two systems.

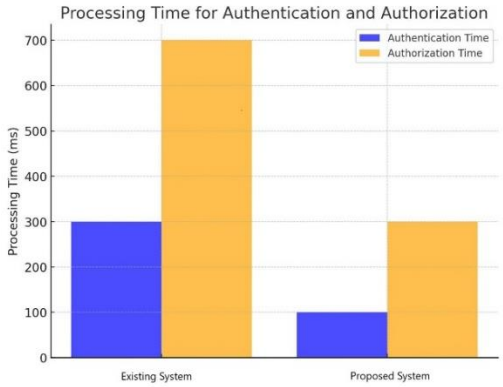


Observations:

- At lower access requests (e.g., 200–600), the difference between the two systems is less pronounced.
- As the number of access requests increases, the proposed system scales better, maintaining a higher throughput. This suggests that the proposed system is more suitable for high-load scenarios.

The graph demonstrates that the proposed system outperforms the existing system in terms of throughput, especially under higher access loads. This improved performance could be due to better resource management, optimized algorithms, or enhanced infrastructure.

The graph below compares the **processing times for authentication and authorization** between the two system.



Observations:

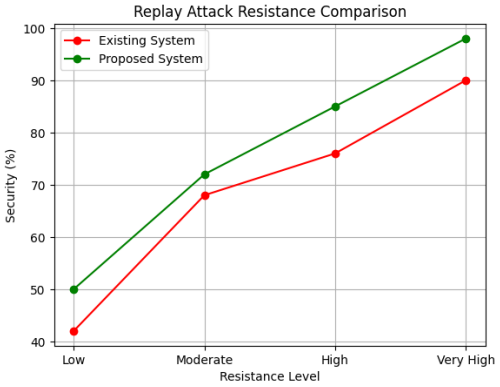
- **Existing System**
  - Authentication Time: ~300 ms.
  - Authorization Time: ~700 ms.
- **Proposed System**

- Authentication Time: ~100 ms (much faster than Scheme [20]).
- Authorization Time: ~300 ms (also much faster than Scheme [20]).

- **Comparison**:
  - **Authentication**: *Proposed System* is approximately 3 times faster.
  - **Authorization**: *Existing System* is approximately 2.3 times faster.

The proposed system significantly outperforms the existing system in both authentication and authorization processing times.
This suggests that **Proposed System** is more efficient and could improve system performance in scenarios where fast processing is critical.

The graph titled "**replay attacks resistance comparison"** compares the resistance level of the proposed system to that of the existing system against replay attacks.

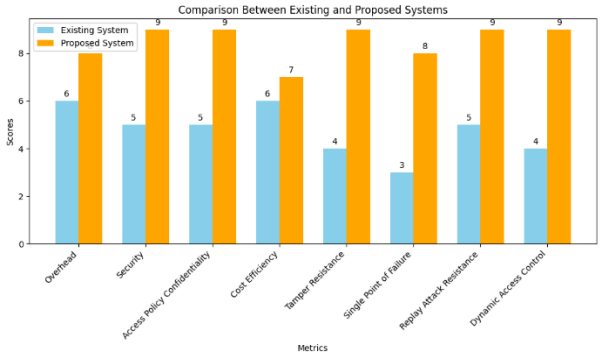


Observations:

- At **Low Resistance Level**, the security of the Proposed System (50%) is slightly higher than the Existing System (40%).
- The Proposed System consistently outperforms the Existing System by a significant margin.
- At the **Very High Resistance Level**, the Proposed System achieves near-perfect security (100%), while the Existing System reaches around 90%.

The **Proposed System** offers consistently better security against replay attacks at all resistance levels compared to the Existing System.

The below graph compares the performance of two systems: the **Existing System** (represented in blue bars) and the **Proposed System** (represented in orange bars), across several key metrics.



6. CONCLUSION AND FUTURE ENHANCEMENT

We have proposed a blockchain-based permission control structure called D2 - IAM system to help strong SSO-approval, dynamic endorsement, and preventive-based induction control with liability in circulated processing. Our structure progressed the cost of SSO-affirmation and endorsement process through the arrangement and execution of canny arrangements and blockchains. As well as achieving high efficiency of check and endorsement, the entry system is shown in the record informational collection which is effortlessness of the chiefs. Furthermore, the mystery of its substance is guaranteed considering the public key encryption. We give the efficiency assessment and preliminary to show that D 2 - IAM is capable basically and its presentation beats existing works. For future works, it is a need to devise the checking on show to support the uprightness of access techniques arranged on cloud. Notwithstanding the way that the game plans are mixed, the attestation of their dependability is at this point essential. The public cloud analyzing systems are worth to research. Additionally, the gathering of decentralized accumulating platforms, such as Inter Planetary File System (IPFS) for storing the policies, PII database can be used to replace the general cloud storage since IPFS provides more efficient file handling with data indexing. Finally, it is worth to develop the anomaly detection method based on machine learning to detect the authentication protocol attack or the misuse of the SSO authentication ticket.

REFERENCES

[1] S. Fugkeaw, P. Manpanpanich, and S. Juntapremjitt, ‘‘Exploiting X.509 certificate and multi-agent system architecture for role-based access control and authentication management,’’ in Proc. 7th IEEE Int. Conf. Comput. Inf. Technol. (CIT), Oct. 2007, pp. 733–738.
[2] The Open ID Connect. Accessed: Jan. 14, 2023. [Online]. Available: https://openid.net/connect/
[3] F. F. Moghaddam, P. Wieder, and R. Yahyapour, ‘‘A policy-based identity management schema for managing

accesses in clouds,'' in Proc. 8th Int. Conf. Netw. Future (NOF), Nov. 2017, pp. 91–98.
[4] N. Naik and P. Jenkins, ''A secure mobile cloud identity: Criteria for effective identity and access management standards,'' in Proc. 4th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud), Mar. 2016, pp. 89–90.
[5] S. Wang, R. Pei, and Y. Zhang, ''EIDM: A Ethereum-based cloud user identity management protocol,'' IEEE Access, vol. 7, pp. 115281–115291, 2019.
[6] N. Hossain, M. A. Hossain, M. Z. Hossain, M. H. I. Sohag, and S. Rahman, ''OAuth-SSO: A framework to secure the OAuth-based SSO service for packaged web applications,'' in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng., New York, NY, USA, Aug. 2018, pp. 1575–1578, doi: 10.1109/TRUSTCOM/BIGDATASE.2018.00227.
[7] C. Tang, X. Fu, and P. Tang, ''Policy-based network access and behavior control management,'' in Proc. IEEE 20th Int. Conf. Commun. Technol. (ICCT), Oct. 2020, pp. 1102–1106.
[8] H. Zhou and L. Zhu, ''Research and design of CAS protocol identity authentication,'' in Proc. Int. Conf. Comput. Vis., Image Deep Learn. (CVIDL), Jul. 2020, pp. 384–387.
[9] M. A. Thakur and R. Gaikwad, ''User identity and access management trends in IT infrastructure—An overview,'' in Proc. Int. Conf. Pervasive Comput. (ICPC), Jan. 2015, pp. 1–4.
[10] M. Uddin, S. Islam, and A. Al-Nemrat, ''A dynamic access control model using authorising workflow and task-role-based access control,'' IEEE Access, vol. 7, pp. 166676–166689, 2019.
[11] S. Fugkeaw, P. Manpanpanich, and S. Juntapremjitt, ''A development of multi-SSO authentication and RBAC model in the distributed systems,'' in Proc. 2nd Int. Conf. Digit. Inf. Manage., 2007, pp. 297–302.
[12] L. Hui, Computational Intelligence and Security (Lecture Notes in Computer Science) vol. 3802. Berlin, Germany: Springer, 2005.
[13] L. Chunge, M. Mingji, L. Bingxu, and C. Shuxin, ''Design and implementation of trust-based access control model for cloud computing,'' in Proc. IEEE 5th Adv. Inf. Technol., Electron. Autom. Control Conf. (IAEAC), Mar. 2021, pp. 1934–1938.
[14] B. Cusack and E. Ghazizadeh, ''Evaluating single sign-on security failure in cloud services,'' Bus. Horizons, vol. 59, no. 6, pp. 605–614, Nov. 2016.
[15] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, ''Cecoin: A decentralized PKI mitigating MitM attacks,'' Future Gener. Comput. Syst., vol. 107, pp. 805–815, Jun. 2020.
[16] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, ''PTAS: Privacypreserving thin-client authentication scheme in blockchain-based PKI,'' Future Gener. Comput. Syst., vol. 96, pp. 185–195, Jul. 2019.
[17] L. Xiong, F. Li, S. Zeng, T. Peng, and Z. Liu, ''A blockchain-based privacyawareness authentication scheme with efficient revocation for multiserver architectures,'' IEEE Access, vol. 7, pp. 125840–125853, 2019, doi: 10.1109/ACCESS.2019.2939368.
[18] S. Wang, X. Wang, and Y. Zhang, ''A secure cloud storage framework with access control based on blockchain,'' IEEE Access, vol. 7, pp. 112713–112725, 2019, doi: 10.1109/ACCESS.2019.2929205.
[19] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, ''AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud,'' IEEE Access, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.
[20] Y. Ping and H. Sato, ''A decentralized framework enabling privacy for authorizable data sharing on transparent public blockchains,'' in Proc. Int. Conf. Algorithms Archit. Parallel Process., Dec. 2021, pp. 693–709.
[21] J. Viega, ''Practical random number generation in software,'' in Proc. 19th Annu. Comput. Secur. Appl. Conf., Las Vegas, NV, USA, 2003, pp. 129–140, doi: 10.1109/CSAC.2003.1254318.
[22] PBC (Pairing-Based Cryptography) Library. Accessed: Oct. 20, 2022. [Online]. Available: https://crypto.stanford.edu/pbc/
[23] G. Wood, et al., ''Ethereum: A secure decentralized generalised transaction ledger,'' Ethereum Project Yellow Paper, Tech. Rep. 151, 2014, pp. 1–32.
[24] G. Zhang, T. Li, Y. Li, P. Hui, and D. Jin, ''Blockchain-based data sharing system for AI-powered network operations,'' J. Commun. Inf. Netw., vol. 3, no. 3, pp. 1–8, 2018.
[25] Y. Ding and H. Sato, ''Derepo: A distributed privacy-preserving data repository with decentralized access control for smart health,'' in Proc. 7th IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)/6th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom), Aug. 2020, pp. 29–35.
[26] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, ''TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain,'' IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 5784–5798, Jun. 2020.
[27] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad, and J. Hatin, ''A novel access control method via smart contracts for internet-based service provisioning,'' IEEE Access, vol. 9, pp. 81253–81273, 2021.
[28] S. Fugkeaw, ''Enabling trust and privacy-preserving e-KYC system using blockchain,'' IEEE Access, vol. 10, pp. 49028–49039, 2022.
[29] Y. Fan, X. Lin, W. Liang, J. Wang, G. Tan, X. Lei, and L. Jing, ''TraceChain: A blockchain-based scheme to protect data confidentiality and traceability,''

Software: Pract. Exper., vol. 52, no. 1, pp. 115–129, Jan. 2022, doi: 10.1002/spe.2753.
[30] OAuth 2.0. Accessed: Jan. 14, 2023. [Online]. Available: https://oauth.net/2/
[31] FIDO Alliance. Accessed: Jan. 14, 2023. [Online]. Available: https://fidoalliance.org
[32] M. Al-Zubaidie, Z. Zhang, and J. Zhang, ''PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system,'' Int. J. Environ. Res. Public Health, vol. 16, no. 9, p. 1490, Apr. 2019, doi: 10.3390/ijerph16091490.
[33] J. Park, R. Sandhu, M. Gupta, and S. Bhatt, ''Activity control design principles: Next generation access control for smart and collaborative systems,'' IEEE Access, vol. 9, pp. 151004–151022, 2021, doi: 10.1109/ACCESS.2021.3126201.
[34] M. J. H. Faruk, H. Shahriar, M. Valero, S. Sneha, S. I. Ahamed, and M. Rahman, ''Towards blockchain-based secure data management for remote patient monitoring,'' in Proc. IEEE Int. Conf. Digit. Health (ICDH), Sep. 2021, pp. 299–308.
[35] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, ''Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment,'' IEEE Access, vol. 10, pp. 36978–36994, 2022, doi: 10.1109/ACCESS.2022.3164081.
[36] J. Wang, J. Chen, N. Xiong, O. Alfarraj, A. Tolba, and Y. Ren, ''S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT,'' ACM Trans. Internet Technol., Feb. 2022, doi: 10.1145/3511902.
[37] P. Tsankov, A. Dan, D. Drachsler-Cohen, A. Gervais, F. Buenzli, and M. Vechev, ''Securify: Practical security analysis of smart contracts,'' in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2018, pp. 67–82.
[38] M. Rodler, W. Li, G. O. Karame, and L. Davi, ''Sereum: Protecting existing smart contracts against re-entrancy attacks,'' in Proc. Netw. Distrib. Syst. Secur. Symp., 2019.
[39] E. Erdem and M. T. Sandikkaya, ''OTPaaS—One time password as a service,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 3, pp. 743–756, Mar. 2019, doi: 10.1109/TIFS.2018.2866025.
[40] X. Yang, X. Yi, S. Nepal, I. Khalil, X. Huang, and J. Shen, ''Efficient and anonymous authentication for healthcare service with cloud based WBANs,'' IEEE Trans. Services Comput., vol. 15, no. 5, pp. 2728–2741, Sep. 2022, doi: 10.1109/TSC.2021.3059856.
[41] R. Vinoth, L. J. Deborah, P. Vijayakumar, and B. B. Gupta, ''An anonymous pre-authentication and post-authentication scheme assisted by cloud for medical IoT environments,'' IEEE Trans. Netw. Sci. Eng., vol. 9, no. 5, pp. 3633–3642, Sep. 2022, doi: 10.1109/TNSE.2022.3176407.
[42] Ethereum Foundation. (2020). Vyper Documentation. Accessed: Jan. 14, 2022. [Online]. Available: https://vyper.readthedocs.io/en/latest/?badge=latest
[43] F. Wang, L. Xu, J. Li, and K.-K.-R. Choo, ''Lightweight public/private auditing scheme for resource-constrained end devices in cloud storage,'' IEEE Trans. Cloud Comput., vol. 10, no. 4, pp. 2704–2716, Oct. 2022, doi: 10.1109/TCC.2020.3045806.
[44] X. Li, S. Liu, R. Lu, M. K. Khan, K. Gu, and X. Zhang, ''An efficient privacy-preserving public auditing protocol for cloud-based medical storage system,'' IEEE J. Biomed. Health Informat., vol. 26, no. 5, pp. 2020–2031, May 2022, doi: 10.1109/JBHI.2022.3140831.