JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

AN EFFECTIVE PRIVACY-PRESERVING BLOCKCHAIN-ASSISTED SECURITY PROTOCOL FOR CLOUD- BASED DIGITAL TWIN ENVIRONMENT

Dr. V Priya, S.B Sakthi Sridhar, M Sanjay Babu, A Yukeshkumar
Professor, Student, Student, Student, Student
Department of Computer Science and Engineering
Paavai Engineering College, Namakkal, Tamilnadu, India-637018.

Abstract*—*Although cloud storage provides convenient data outsourcing services, an untrusted cloud server frequently threatens the integrity and security of the outsourced data. Therefore, it is extremely urgent to design security schemes allowing the users to check the integrity of data with acceptable computational and communication overheads. In this paper, we first propose a public data integrity verification scheme based on the algebraic signature and elliptic curve cryptography. This scheme not only allows the third party authority deputize for users to verify the outsourced data integrity, but also resists malicious attacks such as replay attacks, replacing attack and forgery attacks. Data privacy is guaranteed by symmetric encryption. Furthermore, we construct a novel data structure named divide and conquer hash list, which can efficiently perform data updating operations, such as deletion, insertion, and modification. Compared with the relevant schemes in the literature, security analysis and performance evaluations show that the proposed scheme gains some advantages in integrity verification and dynamic updating.

Keywords—blockchain,cloudbased, digial twin system, Python, security protocol.

I. INTRODUCTION

The proliferation of cloud-based digital twin systems has introduced new dimensions of efficiency and functionality across various industries. However, the inherent vulnerabilities in cloud environments pose significant privacy and security challenges. To address these concerns, this paper proposes a novel privacy-preserving blockchain-assisted security protocol tailored for cloud-based digital twin environments. The protocol leverages the immutable and decentralized nature of blockchain technology to enhance the security and privacy of digital twin data. By utilizing cryptographic techniques such as homomorphic encryption [1] and zero-knowledge proofs, sensitive data can be securely stored and processed while preserving user privacy. Additionally, smart contracts are employed to enforce access control policies and ensure data integrity within the decentralized network. Furthermore, the protocol incorporates a dynamic consensus mechanism to mitigate the risk of data tampering and unauthorized access. Through a distributed consensus process, the protocol ensures that only valid transactions are added to the blockchain, thereby maintaining [2] the integrity of the digital twin environment. To evaluate the effectiveness of the proposed protocol, we conducted extensive simulations and performance analyses. The results demonstrate that our protocol achieves robust security guarantees while minimizing computational overhead and latency. In conclusion, our proposed privacy-preserving blockchain-assisted security protocol offers a comprehensive solution to the privacy and security challenges [3] [6] faced by cloud-based digital twin environments. By leveraging blockchain technology and cryptographic techniques, organizations can safeguard sensitive data, maintain user privacy, and ensure the integrity of their digital twin systems in an efficient and scalable manner.

II. OBJECTIVE

The objective of an effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environments is to establish a robust framework that safeguards sensitive data while maintaining integrity and confidentiality. By integrating blockchain technology, the protocol aims to ensure transparent and immutable record-keeping, enhancing accountability and trust. Efficiency optimization is paramount to minimize computational overhead and resource consumption, while seamless compliance with regulations and interoperability with existing systems enable smooth integration and legal adherence. Ultimately, the protocol seeks to empower users with control over their data privacy while fortifying the security posture of digital twin environments against evolving cyber threats [4] [5].

III. OVERVIEW OF THE PROJECT

The project aims to design and implement a cutting-edge privacy-preserving blockchain-assisted security

protocol for cloud-based digital twin environments. It involves comprehensive research into existing security vulnerabilities and privacy concerns within such ecosystems.

Key components of the project include the development of novel cryptographic techniques tailored for digital twin environments, the design of consensus mechanisms optimized for scalability and performance, and the integration of privacy-enhancing technologies to enable selective disclosure of information.

IV. Module Description

A. Login

Allows the administrator to securely log into the system using valid credentials. Logs login attempts, authentication events, and access control activities for auditing and monitoring purposes. Provides real-time monitoring and alerts for suspicious login activities or security incidents, enabling timely response and mitigation actions.[1] [6]

B. Manage Cloud

provides comprehensive guidance on managing cloud infrastructure specifically tailored to support a privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environments. It covers cloud architecture design, cloud service management, and best practices for integrating blockchain technology with cloud-based digital twins.

C. Upload File

Enables users to upload files from their local devices to the cloud storage system securely. Covers best practices for securely uploading files in cloud-based digital twin environments, focusing on privacy-preserving blockchain-assisted protocols. Learn how to manage, encrypt, and upload files while maintaining security and compliance.

D. Decrypt File

Allows users to decrypt encrypted files stored in the cloud, provided they have the necessary decryption keys. Focuses on secure file decryption in cloud-based digital twin environments, with an emphasis on privacy-preserving blockchain protocols. Learn how to decrypt files while maintaining data integrity and privacy.

E. Stored File

Displays a list of files stored by the user in the cloud storage system, along with relevant details such as file names, sizes, and timestamps. Module explores methods for securely storing files in cloud-based digital twin environments, focusing on blockchain-assisted security protocols. Learn about distributed file storage, data encryption, and access control.

F. Encrypt File

Enables users to encrypt files before uploading them to the cloud, enhancing the security of their data. Securely encrypting files in cloud-based digital twin environments, emphasizing privacy-preserving blockchain-assisted protocols. Explore different [1] encryption algorithms, key management techniques, and how blockchain can ensure encrypted file integrity and secure access control. Learn to implement secure file encryption practices within a blockchain-enhanced cloud infrastructure.

G. Result

Provides users with access to the results of their file management and cryptographic operations, such as encryption/decryption status and any error messages encountered.

V. Software Desciption

Python :

Python is an interpreted high-level programming language for general-purpose programming. Created by Guido van Rossum and first released in 1991, Python has a design philosophy that emphasizes code readability, notably using significant whitespace. It provides constructs that enable clear programming on both small and large scales. In July 2018, Van Rossum stepped down as the leader in the language community. Python features a dynamic type system and automatic memory management.

It supports multiple programming paradigms, including object-oriented, imperative, functional and procedural, and has a large and comprehensive standard library.

Python interpreters are available for many operating systems. CPython, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of Python's other implementations.

Python and CPython are managed by the non-profit Python Software Foundation. Rather than having all of its functionality built into its core, Python was designed to be highly extensible. This compact modularity has made it particularly popular as a means of adding programmable interfaces to existing applications. Van Rossum's vision of a small core language with a large standard library and easily extensible interpreter stemmed from his frustrations with ABC, which espoused the opposite approach. While offering choice in coding methodology, the Python philosophy rejects exuberant syntax (such as that of Perl) in favor of a simpler, less-cluttered grammar. As Alex Martelli put it: "To describe something as 'clever' is not considered a compliment in the Python culture."Python's philosophy rejects the Perl "there is more than one way to do it" approach to language design in favour of "there should be one and preferably only one obvious way to do it".

Python's developers strive to avoid premature optimization, and reject patches to non-critical parts of C Python that would offer marginal increases in speed at the cost of clarity.When speed is important, a Python programmer can move time-critical functions to extension modules written in languages such as C, or use Py a just-in-time compiler. C Python is also available, which translates a Python script into C and makes direct C-level API calls into the Python interpreter. An important goal of Python's developers is keeping it fun to use.

VI. System Architecture

An allocated arrangement of physical elements which provides the design solution for a consumer a system architecture or systems architecture is the conceptual model that defines the structure, behavior, and more views of a system. An architecture description is a formal description

and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system. System architecture can comprise system components, the externally visible properties of those components, the relationships (e.g. the behavior) between them. It can provide a plan from which products can be procured, and systems developed, that will work together to implement the overall system. There have been efforts to formalize languages to describe system architecture; collectively these are called architecture description languages (ADLs).

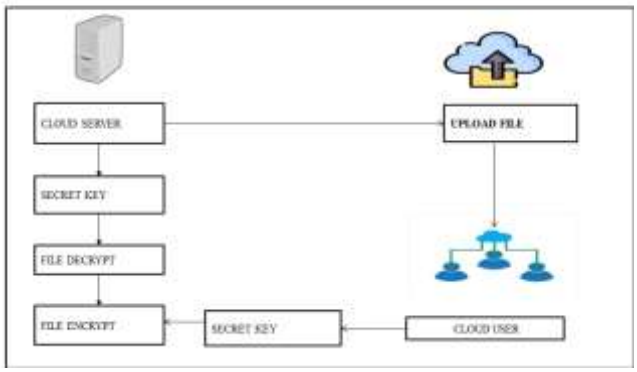

Fig 1: System Architecture

VII. PROTOTYPE MODEL

Fig 2: Web Page and Owner Login Page

Fig3: Owner Details and Upadated List

Fig 4: New Registration Page

Fig 5: New User Login Page and Upload File

Fig 6: New File Upload List

VIII. Conclusion

The development and implementation of an effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environments represent a crucial step forward in addressing the complex challenges surrounding data protection, confidentiality, and integrity in modern digital ecosystems. By placing a strong emphasis on privacy preservation, the protocol aims to safeguard sensitive data associated with digital twins, including personal information, proprietary designs, and operational data, from unauthorized access or disclosure. Integration of blockchain technology offers unparalleled benefits, providing an immutable and transparent ledger for recording transactions and data modifications, thereby enhancing accountability and trust within the ecosystem.

Furthermore, the protocol prioritizes efficiency optimization to minimize computational overhead and resource consumption, ensuring optimal performance without compromising security. Seamless interoperability with existing cloud infrastructure and digital twin platforms enables organizations to integrate the protocol seamlessly into their operations, facilitating compliance with regulatory frameworks such as gdpr, hipaa, and iso/iec 27001. Moreover, the protocol empowers users with granular control over their data privacy, allowing them to specify access permissions, revoke consent, and audit data usage, thereby fostering a culture of transparency and accountability.

IX. References

[1] Al Issa, Huthaifa A, Mustafa Hamzeh Al-Jarah, Ammar Almomani, and Ahmad A1-Nawasrah. “Encryption and decryption cloud computing data based on XOR and genetic algorithm”. *International Journal of Cloud Applications and Computing (IJCAC)* 12, no.1 (2022): 1-10.

[2] Gupta, Ishu, Ashutosh Kumar Singh, Chung-Nan Lee, and Rajkumar Buvya. “Secure data storage and sharing techniques for data protection in cloud environments: A systematic review, analysis, and future directions”. *IEEE Access* 10 (2022): 71247-71277.

[3] Khan, Suleman, Abdullah Gani, Ainuddin Wahid Abdul Wahab, Salman Iqbal, Ahmed Abdelaziz, Omar Adil Mahdi, Abdelmuttlib Ibrahim Abdallaahmed et al. “Towards an applicability of current network forensics for cloud networks: A SWOT analysis”. *IEEE Access* 4 (2016): 9800-9820.

[4] Li, Tao, Baoxiang Du, and Xiaowen Liang. “Image encryption algorithm based on logistic and two-dimensional Lorenz”. *IEEE Access* 8 (2020): 13792-13805.

[5] Li, Weniuan Jian Cao, Keyong Hu, Jie Xu, and Rajkumar Buvya. “A trust-based agent learning model for service composition in mobile cloud computing environments”. *IEEE Access* 7 (2019): 34207-34226.

[6] B. Piascik, J. Vickers, D. Lowry, S. Scotti, J. Stewart, and A. Calomino,‘‘Materials, structures, mechanical systems, and manufacturing roadmap,’’ NASA, Washington, DC, USA, Tech. Rep. TA 12, 2012.

[7] M. Grieves and J. Vickers, ‘‘Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems,’’ in Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches. Cham, Switzerland: Springer, 2017, pp. 85–113.

[8] H. Laaki, Y. Miche, and K. Tammi, ‘‘Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery,’’ IEEE Access, vol. 7, pp. 20325–20336, 2019.

[9] H. Wang and J. Zhang, ‘‘Blockchain based data integrity verification for large-scale IoT data,’’ IEEE Access, vol. 7, pp. 164996–165006, 2019.

[10] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, ‘‘Blockchain data-based cloud data integrity protection mechanism,’’ Future Gener. Comput. Syst., vol. 102, pp. 902–911, Jan. 2020.

[11] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, ‘‘Blockchain based data integrity service framework for IoT data,’’ in Proc. IEEE Int. Conf. Web Services (ICWS), Jun. 2017, pp. 468–475.

[12] S. Son, D. Kwon, J. Lee, S. Yu, N.-S. Jho, and Y. Park, ‘‘On the design of a privacy-preserving communication scheme for cloud-based digital twin environments using blockchain,’’ IEEE Access, vol. 10, pp. 75365–75375, 2022.

[13] T.-Y. Wu, Y.-Q. Lee, C.-M. Chen, Y. Tian, and N. A. Al-Nabhan,‘‘An enhanced pairing-based authentication scheme for smart grid communications,’’ J. Ambient Intell. Humanized Comput., vol. 2021, pp. 1–13, Jan. 2021.

[14] S. Khatoon, S. M. M. Rahman, M. Alrubaian, and A. Alamri, ‘‘Privacypreserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment,’’ IEEE Access, vol. 7, pp. 47962–47971, 2019.

[15] A. Sengupta, A. Singh, P. Kumar, and T. Dhar, ‘‘A secure and improved two factor authentication scheme using elliptic curve and bilinear pairing for cyber physical systems,’’ Multimedia Tools Appl., vol. 16, pp. 1–24, Jul. 2022.