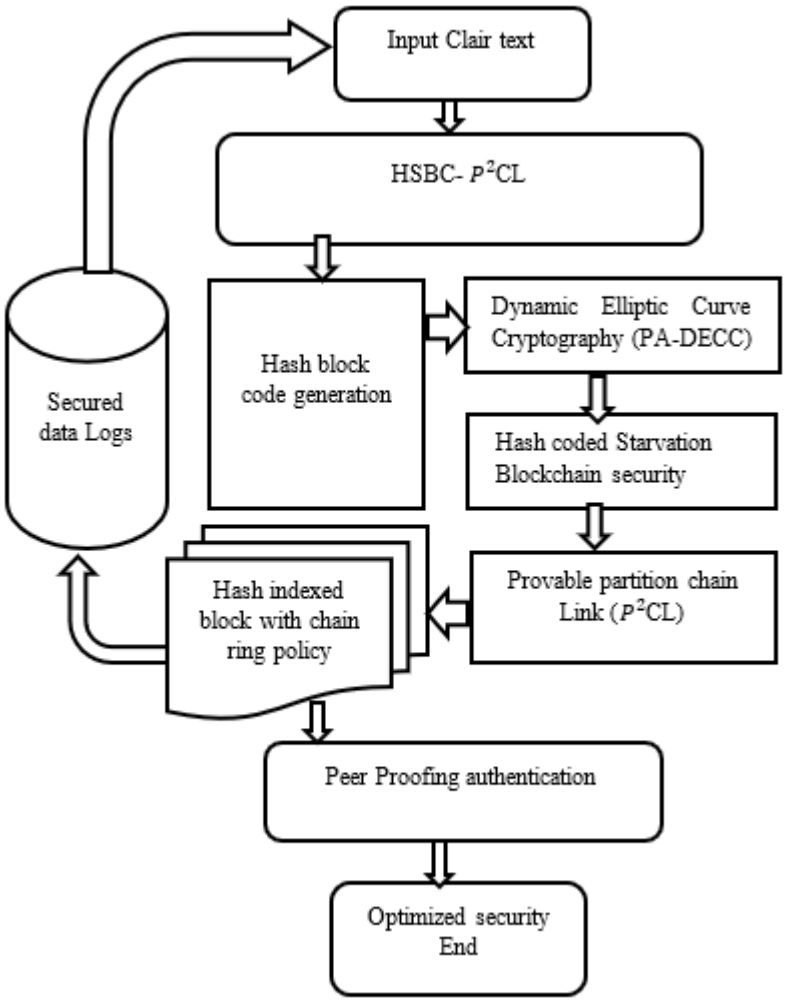
Secure Data Transactions based on Hash Coded Starvation Blockchain Security using Padded Ring Signature-ECC for Network of Things



PDF (https://ijritcc.org/index.php/ijritcc/article/view/5986/5631)

DOI: https://doi.org/10.17762/ijritcc.v11i1.5986 (https://doi.org/10.17762/ijritcc.v11i1.5986)

Keywords:

Blockchain security, ECC cryptography, Padded Ring signature, controller node policy, Network of things

V. Vijayalakshmi
Research Scholar, Department of Computer Science, VISTAS, Chennai – 600117

K. Sharmila
Research Advisor and Associate Professor, Department of Computer Science, VISTAS, Chennai – 600117

Abstract

Blockchain is one of the decentralized processes in a worldview that works with parallel and distributed ledger technology, the application process, and service-oriented design. To propose a Secure data Transaction based on Hash coded Starvation Blockchain security using Padded Ring signature-ECC for Network of Things. Initially, the crypto policy is authenticated based on the user-owner shared resource policy and access rights. This creates a Public blockchain environment with a P2P Blockchain network. The owner encrypts the data using optimized ECC through Hash-coded Starvation Blockchain security (HCSBS). This makes the encrypted block's provable partition chain Link (P^2CL). The encrypted blocks are transmitted into the network of nodes monitored by NoT. During the data transmission, the Network of Things monitors the transaction flow to verify the authenticity over the network of nodes. The monitored data be securely stored in transaction Block storage with the hash-indexed block with chain ring policy (HICLP). This creates controller node aggregation over the transaction environment to securely transfer the data to the peer end. The User gets the access Key to decrypt the data with policy aggregated shared resource policy to access the data. The proposed system produces high security as well compared to the previous design.

How to Cite

Vijayalakshmi, V., & Sharmila, K. (2023). Secure Data Transactions based on Hash Coded Starvation Blockchain Security using Padded Ring Signature-ECC for Network of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(1), 53–61. https://doi.org/10.17762/ijritcc.v11i1.5986

More Citation Formats

Issue

Vol. 11 No. 1 (2023): January (2023) Issue (https://ijritcc.org/index.php/ijritcc/issue/view/126)

Section

Articles

References

A. gbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. (2019) "Blockchain technology in healthcare: a systematic review." In Healthcare, Multidisciplinary Digital Publishing Institute, vol. 7, 56, pp. 1-30.

M. Qiu, H. Qiu, H. Zhao, M. Liu and B. Thuraisingham, "Secure Data Sharing Through Untrusted Clouds with Blockchain-enhanced Key Management," 2020 3rd International Conference on Smart BlockChain (SmartBlock), 2020, pp. 11-16, DOI: 10.1109/SmartBlock52591.2020

D. Tosh, S. Shetty, P. Foytik, C. Kamhoua and L. Njilla, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 302-309, DOI: 10.1109/CLOUD.2018

S. Son, J. Lee, M. Kim, S. Yu, A. K. Das, and Y. Park, "Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain," in IEEE Access, vol. 8, pp. 192177-192191, 2020, DOI: 10.1109/ACCESS.2020.3032680.

B. Chen, L. Wu, H. Wang, L. Zhou and D. He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5813-5825, June 2020, DOI: 10.1109/TVT.2019.2959383.

Y. Yang, H. Lin, X. Liu, W. Guo, X. Zheng, and Z. Liu, "Blockchain-Based Verifiable Multi-Keyword Ranked Search on Encrypted Cloud With Fair Payment," in IEEE Access, vol. 7, pp. 140818-140832, 2019, DOI: 10.1109/ACCESS.2019.2943356.

B. Nassif, M. A. Talib, Q. Nasir, H. Albadani and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," in IEEE Access, vol. 9, pp. 20717-20735, 2021, DOI: 10.1109/ACCESS.2021.3054129

S. Wang, X. Wang, and Y. Zhang, "A Secure Cloud Storage Framework with Access Control Based on Blockchain," in IEEE Access, vol. 7, pp. 112713-112725, 2019, DOI: 10.1109/ACCESS.2019.2929205.

S. Wang, Y. Wang and Y. Zhang, "Blockchain-Based Fair Payment Protocol for Deduplication Cloud Storage System," in IEEE Access, vol. 7, pp. 127652-127668, 2019, DOI: 10.1109/ACCESS.2019.2939492.

X. Yang, G. Chen, M. Wang, T. Li, and C. Wang, "Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on Blockchain," in IEEE Access, vol. 8, pp. 158765-158777, 2020, DOI: 10.1109/ACCESS.2020.3020841.

H. Cui, Z. Wan, X. Wei, S. Nepal, and X. Yi, "Pay as You Decrypt: Decryption Outsourcing for Functional Encryption Using Blockchain," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3227-3238, 2020, DOI: 10.1109/TIFS.2020.2973864.

Bahga, Arshdeep, and Vijay K. Madisetti. (2016) "Blockchain platform for the industrial internet of things." Journal of Software Engineering and Applications 9, no. 10, pp. 533-546

Y. Wang and M. He, "CPDS: A Cross-Blockchain Based Privacy-Preserving Data Sharing for Electronic Health Records," 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA), 2021, pp. 90-99, doi: 10.1109/ICCCBDA51879.2021.

S. Liu, J. Yu, Y. Xiao, Z. Wan, S. Wang, and B. Yan, "BC-SABE: Blockchain-Aided Searchable Attribute-Based Encryption for Cloud-IoT," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7851-7867, Sept. 2020, DOI: 10.1109/JIOT.2020.2993231.

K. Lee, "Comments on “Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption”," in IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1299-1300, 1 Oct.-Dec. 2020, DOI: 10.1109/TCC.2020.2973623.

B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in IEEE Access, vol. 9, pp. 57792-57807, 2021, DOI: 10.1109/ACCESS.2021.3073203

M. Thangavel and P. Varalakshmi, "Enabling Ternary Hash Tree Based Integrity Verification for Secure Cloud Data Storage," in IEEE Transactions on Knowledge and Data Engineering, vol. 32, no. 12, pp. 2351-2362, 1 Dec. 2020, DOI: 10.1109/TKDE.2019.2922357.

Nhlabatsi et al., "Threat-Specific Security Risk Evaluation in the Cloud," in IEEE Transactions on Cloud Computing, vol. 9, no. 2, pp. 793-806, 1 April-June 2021, DOI: 10.1109/TCC.2018.2883063.

J. Zhang, R. Lu, B. Wang and X. A. Wang, "Comments on “Privacy-Preserving Public Auditing Protocol for Regenerating-Code-Based Cloud Storage”," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1288-1289, 2021, DOI: 10.1109/TIFS.2020.3032283.

G. Sciumè, E. J. Palacios-García, P. Gallo, E. R. Sanseverino, J. C. Vasquez and J. M. Guerrero, "Demand Response Service Certification and Customer Baseline Evaluation Using Blockchain Technology," in IEEE Access, vol. 8, pp. 139313-139331, 2020, doi: 10.1109/ACCESS.2020.3012781.

Announcements

Call for Papers (https://ijritcc.org/index.php/ijritcc/announcement/view/10)

March 7, 2024
Call for Papers for the New Issue.

Last Date of Submission: July 31st, 2024

Imp. Announcement

(https://ijritcc.org/index.php/ijritcc/announcement/view/6)

April 15, 2022
Dear Authors,
We are feeling proud congratulations to all the contributors of IJRITCC. Because The "International Journal on Recent and Innovation Trends in Computing and Communication" has been accepted for Scopus.

Citation Index (https://scholar.google.co.in/citations?user=2YiCZVsAAAAJ&hl=en)

Citation Indices	All	Since 2018
Citation	5854	3996
h-index	28	23
i10-index	119	72

Acceptance Rate (By Year)

Year	Rate
2019	12.6%
2018	18.3%
2017	16.9%
2016	18.8%
2015	22.9%
2014	28.9%
2013	26.1%

Important Links

Home (https://ijritcc.org/index.php/ijritcc)
Aims and Scope (https://ijritcc.org/index.php/ijritcc/aims_and_scope)

Call for Papers (https://ijritcc.org/index.php/ijritcc/call_for_papers)
Instructions for Authors (https://ijritcc.org/index.php/ijritcc/guidline_for_authors)
Editorial Board (https://ijritcc.org/index.php/ijritcc/about/editorialTeam)
Archive (https://ijritcc.org/index.php/ijritcc/issue/archive)
Download (https://ijritcc.org/index.php/ijritcc/downloads)
Ethics & Policies (https://ijritcc.org/index.php/ijritcc/ethics_and_policies)
Publication Ethics and Publication Malpractice Statement (https://ijritcc.org/index.php/ijritcc/publication_ethics)
Plagiarism Policy (https://ijritcc.org/index.php/ijritcc/plagiarism_policy)
Copyright, Grants and Ownership Declaration (https://ijritcc.org/index.php/ijritcc/copyright_grants_ownership_declaration)
Refund Policy (https://ijritcc.org/index.php/ijritcc/refund_policy)
Open Access Overview (https://ijritcc.org/index.php/ijritcc/open_access_overview)
Open Access License (https://ijritcc.org/index.php/ijritcc/open_access_license)
Permissions (https://ijritcc.org/index.php/ijritcc/permissions)

Downloads

Paper Template (https://ijritcc.org/downloads/Paper_Template.docx)

Indexed by

(https://www.scopus.com/sourceid/21101089961)

(https://hjrs.hec.gov.pk/index.php?r=site%2Fresult&id=1080285#journal_result)

Make a Submission

Make a Submission (https://ijritcc.org/index.php/ijritcc/about/submissions)

Most Viewed Articles Today

Research Paper on Basic of Artificial Neural Network (https://ijritcc.org/index.php/ijritcc/article/view/2920)
3766

Access Android Device Using The FatRat and Metasploit (https://ijritcc.org/index.php/ijritcc/article/view/5481)
2705

A study and Comparative Analysis of HUL and ITC (https://ijritcc.org/index.php/ijritcc/article/view/319)
2360

Predicting Outcomes of Horse Racing using Machine Learning
(https://ijritcc.org/index.php/ijritcc/article/view/8119)
1946

Aspect-Based Sentiment Analysis using Machine Learning and Deep Learning Approaches
(https://ijritcc.org/index.php/ijritcc/article/view/6636)
1366

Contact Us:

Auricle Global Society of Education and Research
Y-18-A, Near Sanskar Play School, Sudarshana Nagar,
Bikaner, Rajasthan (India). Pin 334003
: *editor@ijritcc.org*

Quick Links:

Author's Guideline (https://ijritcc.org/index.php/ijritcc/guidline_for_authors)
Reviewers Guideline (https://ijritcc.org/index.php/ijritcc/guide_to_reviewing)
Peer Review and Publication Policy
(https://ijritcc.org/index.php/ijritcc/review_process)

FAQ's (https://ijritcc.org/index.php/ijritcc/author_faqs)
Privacy Policy (https://ijritcc.org/index.php/ijritcc/about/privacy)
Refund and Cancellation Policy (https://ijritcc.org/index.php/ijritcc/refund-and-cancellation-policies)
Terms and Conditions (https://ijritcc.org/index.php/ijritcc/terms_and_conditions)

ELSEVIER Scopus (https://www.scopus.com/sourceid/21101089961)

Scilit (https://www.scilit.net/journal/2415509)

INDEX COPERNICUS INTERNATIONAL
(https://journals.indexcopernicus.com/search/formjml?q=ijritcc)

Microsoft Academic (https://academic.microsoft.com/journal/2764488870)

Google scholar (https://scholar.google.co.in/citations?user=2YiCZVsAAAAJ)

Academia.edu (http://ijritcc.academia.edu/ijritcc) SCRIBD

(https://www.scribd.com/user/227678342/Editor-IJRITCC) Crossref