



**ABOUT THE
CONFERENCE**

**Conference
schedule**

SUBMISSION

**CALL FOR PAPERS
& PUBLICATION**

COMMITTEE
▼

REGISTRATION

**KEYNOTE
SPEAKERS**

**ABOUT
IEM/UEM
GROUP**

GALLERY

CONTACT

**IRTM
2023**

**SISTER
CONFERENCE**
▼



International Conference On “Interdisciplinary Research in Technology & Management”
19th-21st November 2025, Kozhikode, Kerala, India

IMPORTANT DATES –



Organized by

Institute of Engineering & Management, Kolkata

and

**University of Engineering & Management, Kolkata and
Jaipur**

Along with NIT, Calicut

In association with

**Vijnan Bharati, Vivekananda Vijnan Mission, West Bengal Chapter of Vijnan Bharati
and Vijnan Bharati Mumbai supported by SMART Society, USA.**

And Supported by

SMART Society, USA

WE ARE HONOURED TO HAVE

**19th-21st November,
2025 Conference Dates**

**5th September,
2025 Full paper submission**

**20th October,
2025 Acceptance
Notification**

**5th November,
2025 Camera-ready copy
due**

**5th November,
2025 Presentation
Submission**

**5th November,
2025 Registration**

[Register Here](#)

IRTM 2024



SUBHRADEEP HAZRA <subhradeephazra2003@gmail.com>

[IRTM 2024] Your paper #1571068105 ('A Comprehensive Study of the Correlation Between Blockchain Dynamics and Cybersecurity: Complementing Digital Trust and Security for Cryptocurrency Transactions')

irtm2024-chairs@edas.info <irtm2024-chairs@edas.info>

22 October 2024 at 11:06

To: Indranil Maity <indranil.maity@iem.edu.in>, Snehadri Bhaumik <snehadribhaumik.bkp@gmail.com>, Subhradeep Hazra <subhradeephazra2003@gmail.com>

Dear Dr. Indranil Maity:

Congratulations - your paper #1571068105 ('A Comprehensive Study of the Correlation Between Blockchain Dynamics and Cybersecurity: Complementing Digital Trust and Security for Cryptocurrency Transactions') for IRTM 2024 has been **accepted** and will be presented in the session titled ____.

The reviews are below or can be found at [1571068105](#).

IRTM 2024 1**Comments for reviewers: write at least 100 words regarding this review**

paper can be accepted

IRTM 2024 2**Comments for reviewers: write at least 100 words regarding this review**

accept

Regards,
The conference chairs

A Comprehensive Study of the Correlation between Blockchain Dynamics and Cybersecurity: Complementing Digital Trust and Security for Cryptocurrency Transactions

Indranil Maity

Department of Electronics and
Communication Engineering (ECE)

Institute of Engineering and
Management (IEM)

University of Engineering and
Management (UEM)

Kolkata, West Bengal, India

Email: indrasanu026@gmail.com

Snehadri Bhaumik

Department of Electronics and
Communication Engineering (ECE)

Institute of Engineering and
Management (IEM)

Kolkata, West Bengal, India

Email: snehadribhaumik.bkp@gmail.com

Subhradeep Hazra

Department of Electronics and
Communication Engineering (ECE)

Institute of Engineering and
Management (IEM)

Kolkata, West Bengal, India

Email: subhradeephazra2003@gmail.com

Abstract—In this paper, a critical review has been conducted to address the knowledge gap behind implementing the traditional data tracking system instead of using cloud-based technologies. The focus is on blockchain technology, which has emerged as a highly promising cloud-based technology with high potential. The fundamentals and superiority over traditional systems of this technology are documented here. The two key challenges that are hindering the adoption of such technology in developing countries in recent times are data piracy and different cyber-attacks which can be overcome using cybersecurity remedies. Additionally, a framework was studied and presented consisting of one hashing algorithm (SHA-256) and an encryption algorithm (RSA), implemented to store the transaction details of bitcoin which could help to secure data and safeguard it from any kind of piracy or unknown decryption.

Keywords—Cryptocurrency, SHA-256, RSA, Merkle tree, Hash

I. INTRODUCTION

The most promising data-storing technique in recent times is cloud-based technology. In this system, data is stored in the cloud and encrypted using various algorithms, preventing unauthorized access and intervention [1]. Blockchain, a leading cloud-based technology, is an organized database of entrenched records called blocks which are encrypted using cryptography. These blocks form a chain as a linked list where each block is a record book containing details of tasks in enciphered form which can be data, assets, or transaction history of any cryptocurrency along with the hashing address of the previous block [2]. However, data piracy is one of the most significant problems of this system arising across the globe in recent times. It revolves around unauthorized interventions on data leading to copying, manipulation, monitoring, and distribution of data or a piece of digital information without proper access to the owner [3]. Cybersecurity is one troubleshooting way to secure the interconnected networks among these blocks and encrypted data from unknown and unauthorized access. It comprises scientific methods and layers of encryption to maintain the uniqueness and integrity of data [4].

In this theoretical study, Aguilar et al. critically analyzed the common threats specific to blockchain technologies, including 51% device attacks and various smart contract vulnerabilities. They emphasized various blockchain security schemes encompassing different encryption algorithms and other service protocols [5]. Rathore et al. designed a novel framework encompassing blockchain technology with deep learning algorithms for real-time identification of threats, including data piracy, and proposed a framework to enhance extensive security in Industrial Cyber-Physical Systems (ICPS) [6]. Zhuang et al. critically surveyed the cybersecurity problems faced in smart grid systems, including duplication and unknown tampering of data leading to data manipulation, and hence included blockchain technology to ensure proper and secure data management [7]. Patil et al. critically compared the performance metrics including encoding and decoding speed, size of keys, and security level of various encrypting algorithms like Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) ensuring cybersecurity [8]. Kumar et al. integrated blockchain technology with the Interplanetary File System (IPFS) to create a novel framework for proper data storage ensuring proper authorization and securing the interconnected network [9]. Porkodi et al. formulated a conceptual framework that united the Internet of Things (IoT) and the blockchain technology to ensure reliability and centralized control over secured data [10]. N. Gupta examined specific attack vectors causing severe threats to data in blockchain technology such as double-spending and Sybil attacks and formulated different consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) [11]. Sharma et al. critically analyzed the overview of the fundamental concepts of cryptocurrencies and the importance of blockchain technology in ensuring transparency and security [12].

In this paper, blockchain technology and cybersecurity were deeply reviewed based on their importance, features with probable attacks, and remedies. Also, a parallelism between blockchain technology and cybersecurity was critically analyzed with the help of two cutting-edge algorithms viz, (1) Secure Hash Algorithm-2 (SHA-256) to encrypt the stored data and (2) encryption algorithm (RSA) to generate a pair of private and public keys.

V. CONCLUSION

In this theoretical study, an in-depth analysis was performed to highlight the key concepts of blockchain networks, data piracy, and the growing importance of cybersecurity in maintaining transparency and stability of data. The fundamentals of a blockchain network, a block, act as the basis of any transaction or any communication between two or more users over a particular network. Every block was uniquely identified by a hash address and encrypted using different cryptographic algorithms maintaining data security and ensuring that the complete distributed ledger network of transactions was immune to unauthorized access. A framework for sharing transaction details of bitcoin was reviewed where the SHA-256 algorithm was used to encrypt the details and the RSA algorithm was utilized in the digital signature as a proof of work to hide the users' details.

ACKNOWLEDGMENT

We extend our appreciation to the Institute of Engineering and Management (IEM) for providing a conducive environment for academic exploration.

REFERENCES

- [1] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, and J. Platts, "Cybersecurity, Data Privacy and Blockchain: A Review," Springer Nature Computer Science Journal, vol. 3, article 27, 2022.
- [2] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology Internal Report (NISTIR), pp. 8202, 2018.
- [3] V. Wylde, E. Prakash, C. Hewage, and J. Platts, "Covid-19 Crisis: Is our Personal Data Likely to be Breached?" The 5th Advances in Management and Innovation Conference, 2021.
- [4] Z. Zhao, and G. Chen, "An Overview of Cyber Security for Smart Grid," 27th International Symposium on Industrial Electronics (ISIE), 2018.
- [5] M. Aguilar, J. Fuentes, L. Manzano, and D. Arroyo, "Achieving cybersecurity in blockchain-based systems: A survey," Future Generation Computer Systems, vol. 124, pp. 91-118, 2021.
- [6] S. Rathore, and J. Park, "A Blockchain-Based Deep Learning Approach for Cyber Security in Next Generation Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5522-5532, 2021.
- [7] P. Zhuang, T. Zamir, and H. Liang, "Blockchain for Cyber Security in Smart Grid: A Comprehensive Survey," IEEE Transactions on Industrial Informatics, vol. 17, issue 1, pp. 3-19, 2020.
- [8] P. Patil, P. Narayankar, D. Narayan, and S. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," International Conference on Information Security & Privacy (ICISP), 2015.
- [9] R. Kumar, and R. Tripathi, "Blockchain Based Framework for Data Storage in Peer-to-Peer scheme using Interplanetary File System," Handbook of Research on Blockchain technology, pp. 35-87, 2020.
- [10] S. Porkodi, and D. Kesavaraja, "Integration of Blockchain and Internet of Things (IoT)," Handbook of Research on Blockchain Technology, pp. 61-94, 2020.
- [11] N. Gupta, "A Deep Dive into security and piracy issues of Blockchain Technologies," Handbook of Research on Blockchain Technology, pp. 95-111, 2020.
- [12] D. Sharma, S. Pant, M. Sharma, and S. Brahmachari, "Cryptocurrency mechanisms for Blockchains: Models, Challenges, Characteristics and Applications," Handbook of Research on Blockchain Technology, pp. 323-345, 2020.
- [13] K. Michael, S. Kobran, R. Abbas, and S. Hamdoun, "Privacy, Data Rights and Cybersecurity Technology for Good in the Achievement of Sustainable Development Goals," IEEE International Symposium on Technology in Society (ISTAS) Proceedings Miriam Cunningham and Paul Cunningham (Eds), 2019.
- [14] Z. Wang, L. Sun, and H. Zhu, "Defining Social Engineering in Cybersecurity," IEEE Access, vol. 8, pp. 85094-85115, 2020.
- [15] Devika K. N. and R. Bhakthavatchalu, "Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept," International Conference on Communication and Signal Processing, 2019.
- [16] X. Zhou, and X. Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption," The 6th International Forum on Strategic Technology, 2011.
- [17] N. A. Ugochukwu, S. B. Goyal, A. S. Rajawat, S. M. N. Islam, J. He, and M. Aslam, "An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method," Mathematics, vol. 10, 2022.
- [18] I. Maity, H. Nagasawa, T. Tsuru, and P. Bhattacharyya, "Correlation Between Ammonia Selectivity and Temperature Dependent Functional Group Tuning of GO," IEEE Trans. Nanotechnol., vol. 20, pp. 129-136, Dec. 2020.
- [19] P. Radanliev, "The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse," Financial Innovation, vol. 10, no. 1, 2024.
- [20] I. Maity and P. Bhattacharyya, "Room Temperature Acetone Sensing Performance of rGO-ZnO Nanotubes Binary Hybrid Structure," Sensor Lett., vol. 17, no. 6, pp. 417-422, Jun. 2019.



Certificate of Presenter

This certificate is proudly awarded to

Snehadri Bhaumik

from

Institute of Engineering and Management (IEM) Kolkata

for paper titled

A Comprehensive Study of the Correlation between Blockchain Dynamics and Cybersecurity: Complementing Digital Trust and Security for Cryptocurrency Transactions

at

4TH INTERNATIONAL CONFERENCE ON
**INTERDISCIPLINARY RESEARCH IN
TECHNOLOGY & MANAGEMENT - 2024**
held from 5th-7th December 2024

DR. SATYAJIT CHAKRABARTI
DIRECTOR, INSTITUTE OF
ENGINEERING & MANAGEMENT