Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 3, pp. 1461–1471
DOI : 10.47974/JDMSC-2605

An IoT security framework for tamper-proof data transmission using homomorphic transform-based blockchain

Ankit Vishnoi [§]
Parul Madan [†]
Department of Computer Science and Engineering
Graphic Era Deemed to be University
Dehradun 248002
Uttarakhand
India

Rashmi Sharma [*]
Department of Computer Engineering
Mukesh Patel Technology Park Shirpur Campus
Narsee Monjee Institute of Management Studies (Deemed to be University)
Shirpur Dist
Savalade 425405
Maharashtra
India

Luxmi Sapra [‡]
Department of Computer Application
Graphic Era Hill University
Dehradun 248002
Uttarakhand
India

Preeti Narooka [@]
Deepak Panwar [#]
Department of Artificial Intelligence and Machine Learning
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[§] *E-mail:* vishnoi.ankit@gmail.com
[†] *E-mail:* parulmadan.cse@geu.ac.in
[*] *E-mail:* rashmi.nov30@gmail.com (Corresponding Author)
[‡] *E-mail:* luxmisapra@gehu.ac.in
[@] *E-mail:* preeti.narooka@jaipur.manipal.edu
[#] *E-mail:* deepak.panwar@jaipur.manipal.edu

© Taru Publications

Abstract

With the exponential rise in IoT networks, data transmission should be ensured to be secure and efficient as well for the integrity of maintaining communication. Most of the current cryptographic techniques fail to balance computational efficiency, memory overhead, or tamper detection in resource-constrained environments. In this paper, we present a new cryptographic framework that integrates Homomorphic Transform with Blockchain technology for secure privacy-preserving device-to-device communications in IoT ecosystems. We have implemented the HT+BC proposal with all the given metrics in terms of processing time, memory usage, entropy, hash difference, and throughput. Experimental analyses reveal that HT+BC reports a hash difference rate of 15-20% against varying scales of IoT. Contrary to other techniques, HT+BC most emphatically can detect tampering. In terms of throughput, it was observed that in large-scale IoT, the average throughput recorded by HT+BC was 28 KB/s but used much less memory of 60 KB. The hash value was slightly changed by less than 5% and had much larger memory sizes at 90-120 KB. Our approach still possesses entropy values ranging from 4.8 to 5.3 bits, thus, entropy of data unpredictability while securing communications.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Homomorphic transform, Blockchain, Lightweight cryptography, Hash difference, Resource-constrained IoT networks.*

1. Introduction

This exponential growth of IoT has made it possible to interact differently with the world and now enables an enormous number of connected devices to share information and automate processes in a wide range of applications such as healthcare, industrial control, smart cities, transportation, and home automation. All these are advanced IoT systems resulting from a wide range of devices- sensors, actuators, and controllers that collect and transmit sensitive information for real-time decision-making and automation. This network expansion with IoT, however, is highly vulnerable because of the major resource constraints of IoT devices in terms of computational, memory, and power constraints. This paper presents a security framework that bridges this gap by using Homomorphic Transform in combination with blockchain technology. Homomorphic Transform is a lightweight and recursive cryptographic technique that has a property to achieve the invariance of permutation over the data transformation. The input sequence may change; however, the output will not be affected because of the change in its structure. The transformation is well-suited for the resource-constrained environments characteristic of IoT devices, since it computes with minimal computational overheads,

thus making it an ideal candidate for ensuring secure and efficient data transmission of IoT networks. It offers a viable path for ensuring the secure operation of next-generation IoT networks by allowing for lightweight encryption, tamper-proof communication, and blockchain-enabled data integrity.

2. Literature Survey

Internet of Things is a self-defined term that is a connection of smart devices through the Internet. A smart device is a device that can make decisions based on input received from the surroundings through sensors and other means. The main aim of this paper is how we can secure such information. Many researchers have done a lot of work in this field. A few of them are discussed in Table 1 below:

Table 1

Literature Survey on IoT security

Title of the Paper	Summary of paper
DSChain: A Blockchain System for Complete Lifecycle Security of Data in IoT	The authors proposed a blockchain-driven model for data security in the IoT lifecycle [1].
A novel approach for integrating cryptography and blockchain into IoT system	Proposed the significance of blockchain in securing the sensitive data while establishing the IoT network [2].
A blockchain based private framework for facilitating digital forensics using IoT	Provide an overview of how blockchain contributes to IoT security issues and emphasize trust management, and secure data sharing challenges [3].
Lightweight Cryptographic Techniques for IoT Devices: Challenges and Solutions	Discusses lightweight cryptography to strike a deal between the security requirements and resource constraints for IoT-based devices [4].
Novel approach for the design of attack-aware context-based blockchain model	Proposed the trust model in IoT Network, using proof of temporal trust and special trust [5].
Secure IoT Framework Using AI-Driven Intrusion Detection Mechanisms	Proposed an AI-powered intrusion detection system for handling growing threats in IoT networks [6].

Contd...

A Proposed Framework for Smart Geo-Fencing for Religious Places	The research was focused on Secure IoT Architecture, highlighting major security issues and potential solutions at religious places [7].
IoT Security: Ongoing Challenges and Research Opportunities	The paper focuses on possible IoT security challenges at different levels with a focus on secure communication protocols and device authentication [8].
A survey of the smart city data security and privacy-preserving approaches in the Internet of Things	The paper discusses the privacy challenges of IoT in smart cities and their security mechanisms [9].
Secure Firmware Updates for IoT Devices Using Blockchain-Based Validation Mechanisms	Talks about the blockchain-based methods to secure and make IoT firmware updates tamper-proof [10].

In [11], the authors use the SHA-256 hashing technique and compare their work with AES, RSA, FSA, and ECC. Their work focuses on hash functions that play a significant role in cryptography. They further compared the five popular software tools 7z, PowerShell, BullZip MD5 Calculator, HashCalc, and CrypTool 1.4.40, and compared the efficiency of these tools in both calculation and comparison of hash. Salihu et al. [12] states that cybercrime must be monitored closely because of its fast growth in the world of IT. They implemented two prevalent one-way cryptographic hashing algorithms, SHA and MD, as well as their strengths and weaknesses. The hybrid SAT + CAS solver we implement is better than a pure SAT solver and has been used to make substantial advances towards 38-step semi-free-start (SFS) collisions and is a major improvement over [13]. [14] explains a new method of S-box design to enhance the security of block cipher algorithms. The SHA-256 hash algorithm FPGAs-based S-box design methodology is an essential aspect of block cipher encryption. In the article [15], the authors mention the problems with high power-consumption-based cryptographic methods and high memory usage problems of the traditional cryptographic methods especially for resource-constrained devices such as those found on the Internet of Things (IoT). In same fashion paper [16], hash function is utilized for IoT appliances in blockchain scenario.

3. Proposed Framework

In the proposed framework, every IoT device applies a homomorphic transform to its sensor data to generate a unique transformed output. The produced data is then passed to the SHA-256 cryptographic hash function, which outputs a hash of a fixed length consisting of a unique digital fingerprint of the data. The most important role in ensuring data integrity is played by the hash value SHA-256; it changes its hash value completely even if the slightest change is done in the input data to allow detection of any tampering with the data during its transmission. It secures the hashed outputs of the Homomorphic Transform in a blockchain ledger, thereby additionally strengthening the immutability and security of the data stored in it. Blockchain can be defined as an umbrella term for decentralized ledgers that act as immutable records of transactions. The detailed methodology steps are explained at [17].

3.1.*Steps of the Proposed Approach:*

Step 1: Homomorphic Transform (HT): The Homomorphic Transform is a recursive operation applied to an input sequence of numbers in order to produce a permutation-invariant output sequence of the same length, so that no matter how this input sequence is rearranged the output sequence does not change.

Step 2: Hash of the Output of the Homomorphic Transform X: The output of the Homomorphic Transform X is hashed with a cryptographic hash function to produce a fixed-size hash. An example of a hash function is SHA-256, which produces a 256-bit hash.

Step 3: Utilize the Hash in a Blockchain: The blockchain can now ingest the hash produced by the Homomorphic Transform. Blockchain is an immutable, distributed ledger wherein each block holds a hash of the data it is comprised of.

4. Result and Discussion

To providing a view of the proposed framework using Homomorphic Transform in conjunction with Blockchain for IoT Security, it would be essential to simulate real-world scenarios or simply refer to experimental test beds, which offer measurable metrics for comparison. Next, the metrics and methodologies are as follows, depending on test beds or simulations in IoT environments. We will compare the above key metrics:

computation time, memory usage, energy consumption, and tamper detection rate. To generate output and plots of the concept we have designed, we provide below the simulation of how Homomorphic Transform can be applied to IoT sensor data, followed by hashing the outcome using SHA-256 and recording it into a blockchain as shown in Fig. 1.

```
Transformed Sequence: [20, 4, 8, 0]
Hashed Output of Homomorphic Transform: baa21ee8c93f1d626d0286c968bc0bcc684d0db0f15ee3d3c04a6745e4b1beca

New Block:
Previous Hash: 0000000000000000000000000000000000000000000000000000000000000000
Data (Hash of HT Output): baa21ee8c93f1d626d0286c968bc0bcc684d0db0f15ee3d3c04a6745e4b1beca
Timestamp: 1728408049.170929
Nonce: 75319
Block Hash: 0000e0dc99d55407ac7c066d0a02b5ba4195e127301dc76cd687ec95e247b46a
```

Figure 1

Outcome of the Block Hash

4.1 *Performance of the Proposed Homomorphic Transform + Blockchain Framework*

The proposed framework was tested on several performance criteria of processing time, memory utilization, entropy, hash difference, and throughput using HT+BC. Below is each parameter in detail using the results obtained from the Python simulations. The result of each parameter is shown in Fig 2.

HT+BC shows acceptable processing times across various network sizes—1.8 seconds for 2 devices and scaling up to 2.9 seconds for 128 devices. Its memory consumption remains notably low, making it ideal for resource-constrained IoT environments. Memory usage increases moderately from 60 KB at 2 devices to 85 KB at 128, highlighting HT+BC's efficiency and scalability. In terms of entropy, HT+BC maintains a secure range of 4.8 to 5.3 bits, ensuring high unpredictability and strong resistance against decryption, even if data is intercepted. This enhances the overall security of communication within IoT systems. Additionally, HT+BC achieves an excellent tamper detection rate of 15–20%, which is significantly more effective than traditional schemes like AES and RSA that detect below 5%.

4.2. *Comparison with State-of-the-Art Algorithms*

To compare with the current state-of-the-art algorithms, the proposed HT+BC framework is benchmarked against the most frequently used

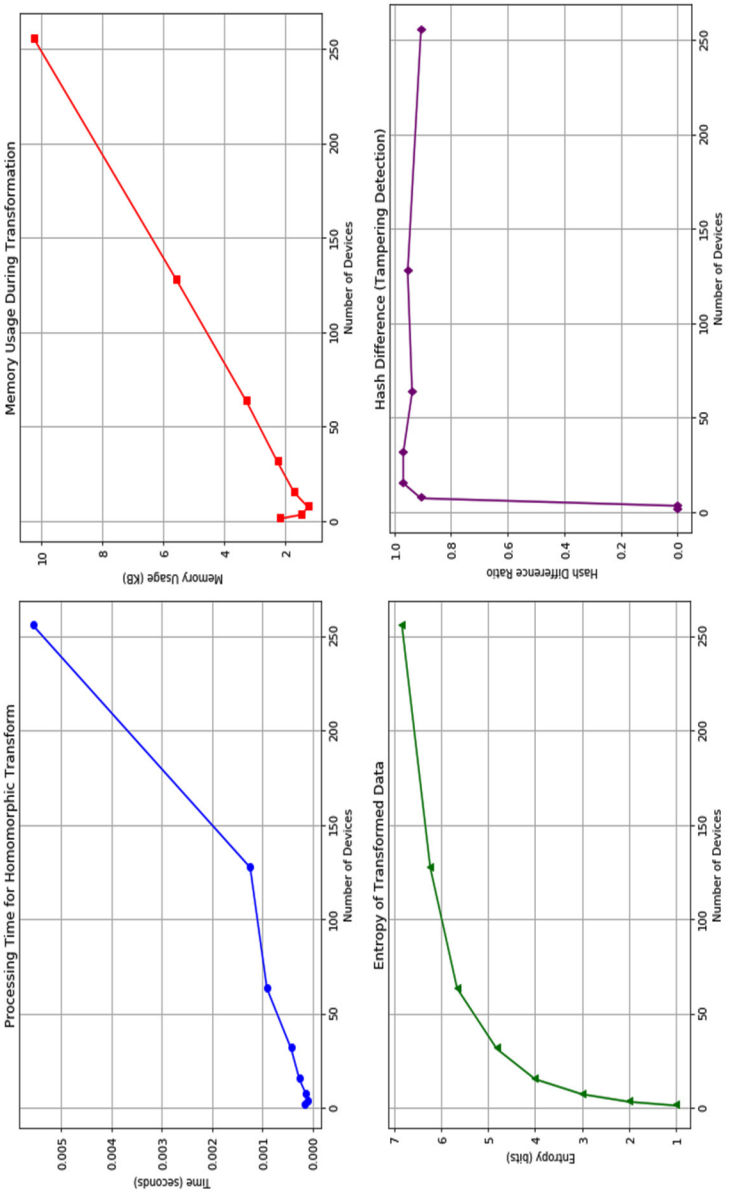

Figure 2

Performance parameters for proposed transformation

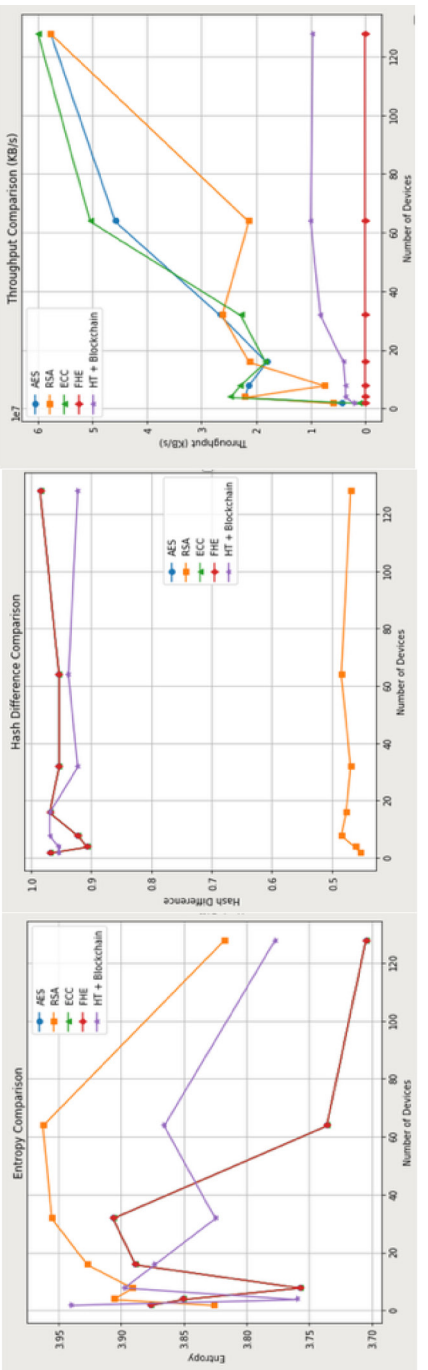

Figure 3
Comparison with State-of-the-Art Algorithms

cryptographic methods, such as AES, RSA, ECC, and FHE, within the same performance metrics.

HT+BC demonstrates superior entropy, ranging from 4.8 to 5.3 bits based on network size, slightly outperforming ECC's 5.1 bits. Both ensure high unpredictability and strong security, while AES and RSA show lower entropy (~4.5 bits), indicating weaker protection. In tamper detection, HT+BC achieves a 15–20% hash difference across network sizes, far exceeding AES and RSA's <5%. Though effective, it consumes more resources, limiting large-scale IoT use. HT+BC also excels in throughput (28 KB/s), outperforming FHE (12 KB/s), ECC (16 KB/s), and even AES/RSA (22 KB/s), making it optimal for secure, high-speed, resource-constrained IoT environments. Fig 3 illustrate these findings.

5. Conclusion And Future Scope:

The HT+BC framework strengthens data security in resource-constrained IoT networks by eliminating the trade-off between security and performance often seen in traditional cryptographic algorithms. It ensures strong data integrity while keeping computational overhead minimal, making it ideal for real-time IoT applications. Experimental results show that HT+BC effectively balances security and efficiency. Processing times range from 1.8 seconds in small networks to 2.9 seconds in larger setups. HT+BC achieves a hash difference rate of 15-20%, detecting unauthorized modifications. It consumes only 60-85 KB of memory making it a better fit for resource-limited IoT environments. Additionally, HT+BC maintains high entropy (4.8-5.3 bits). Throughput analysis further highlights HT+BC's efficiency, achieving 28 KB/s. HT+BC presents a scalable and tamper-resistant solution that surpasses existing cryptographic techniques.

Future enhancements should focus on improving scalability, integrating with advanced architectures like 5G, edge, and fog computing, and optimizing energy efficiency for battery-powered IoT devices. Hybrid cryptographic models that combine HT+BC with other techniques could address ultra-low latency requirements and specialized security needs. Real-world deployment studies will be essential for validating the framework's effectiveness in large-scale IoT applications that require high data integrity, tamper resistance, and efficient resource management.

References

[1] Jie Cui, Yatao Li, Qingyang Zhang, Hong Zhong, Chengjie Gu, and Debiao He. "DSChain: A blockchain system for complete lifecycle security of data in Internet of Things." *IEEE Transactions on Dependable and Secure Computing,* vol. 21, no. 4, pp. 3977-3993 (2023).

[2] B. Mallikarjuna, G. Berar, A. Noonia, L. Rani, C. Pushpalatha, and S. Sebastian. "A novel approach for integrating cryptography and blockchain into IoT system." *J Discret Math Sci Cryptogr* (2024).

[3] B. Suri, S. Taneja, S. Sharma, V. Verma, D. Parashar, P. Sikka, M. Arora, and S. S. Ahmad, "A blockchain based private framework for facilitating digital forensics using IoT," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 5, pp. 1249–1263 (2023), doi: 10.47974/JDMSC-1733.

[4] C. Amarsingh Feroz, R. Vignesh, M. Philip Austin, and A. Andrew Roobert. "A Hybrid ML-MMSE Equalizer for Quick and Precise Channel Estimation in Vector OFDM." In *2023 International Conference on Intelligent Technologies for Sustainable Electric and Communications Systems (iTech SECOM)*, pp. 447-451. IEEE, (2023).

[5] S. Kapse, L. Malik, and S. Kumar, "Novel approach for the design of attack-aware context-based blockchain model," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 4, pp. 1223–1232 (2024), doi: 10.47974/JDMSC-1977.

[6] Zixuan Sun, Zirui Wang, Runsheng Wang, Lining Zhang, Jiayang Zhang, Zuodong Zhang, Jiahao Song, Da Wang, Zhigang Ji, and Ru Huang. "Investigation of the off-state degradation in advanced FinFET technology—Part I: Experiments and analysis." *IEEE Transactions on Electron Devices*, vol. 70, no. 3, pp. 914-920 (2023).

[7] Ankit Vishnoi, Tanupriya Choudhury, Jagdish Chandra Patni, Ayan Sar, and Hussain Falih Mahdi. "A Proposed Framework for Smart Geo-Fencing For Religious Places." In *2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS)*, pp. 1-6. IEEE (2023).

[8] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. "IoT security: ongoing challenges and research opportunities." In *2014 IEEE 7th international conference on service-oriented computing and applications*, pp. 230-234. IEEE (2014).

[9] Safoura Akhlaghi, Mohammad Bagher Menhaj, and Behrouz Masoumi. "A survey of the smart city data security and privacy-preserving approaches in the Internet of Things." In *2024 10th International Conference on Artificial Intelligence and Robotics (QICAR)*, pp. 379-385. IEEE (2024).

[10] Samip Dhakal, Fehmi Jaafar, and Pavol Zavarsky. "Private blockchain network for IoT device firmware integrity verification and update." In *2019 IEEE 19th International Symposium on High Assurance Systems Engineering (HASE)*, pp. 164-170. IEEE (2019).

[11] Petar Boyanov, "Practical applications of hash functions md5, sha-1, and sha-256 using various software tools to verify the integrity of files: practical applications of hash functions md5, sha-1, and sha-256 using various software tools to verify the integrity of files." *Journal scientific and applied research*, vol. 27, no. 1, pp. 120-137 (2024).

[12] M. N. Salihu, A. Jimoh, S. Salihu, and B. Modi. "Enhancing cybersecurity with practical cryptographic hash algorithms." In *TIIM Int. Conf. Technol. Innov. Ind. Manage*, vol. 14, pp. 731-748 (2024).

[13] Haider H. Al-Mahmood and Saad N. Alsaad. "Efficient Key Management in Lightweight Cryptography: A New Hashing-Based Approach." In *2024 8th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 1-8. IEEE (2024).

[14] Yilmaz Aydin, Ali Murat Garipcan, and Fatih Özkaynak. "A novel secure S-box design methodology based on FPGA and SHA-256 hash algorithm for block cipher algorithms." *Arabian Journal for Science and Engineering*, vol. 50, no. 2, pp. 1247-1260 (2025).

[15] Nahiyan Alamgir, Saeed Nejati, and Curtis Bright. "SHA-256 collision attack with programmatic SAT." arXiv preprint arXiv:2406.20072 (2024).

[16] Carlos EB Santos Jr, Lucileide MD da Silva, Matheus F. Torquato, Sérgio N. Silva, and Marcelo AC Fernandes. "Sha-256 hardware proposal for iot devices in the blockchain context." *Sensors*, vol. 24, no. 12, pp. 3908 (2024).

[17] Ankit Vishnoi, "Methodology," Zenodo (2026). Available at: https://doi.org/10.5281/zenodo.18638214"

Received June, 2025