International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Analysis of Blockchain Protocol Using Machine Learning for Lightweight Cryptography

Nilesh Goriya[1], Viral Patel[2], Upendra Bhoi[3], Nainesh Nagekar[4]

Submitted: 05/05/2024 **Revised**: 18/06/2024 **Accepted**: 25/06/2024

Abstract: Anonymity, security, immutability, and audibility are four of blockchain's important properties that have garnered a lot of attention recently. The Internet of Things is only one of many non-monetary uses for blockchain technology. While present-day blockchain technology works well under more ideal conditions, it runs into problems when used in places with limited resources. In such limited contexts, conventional cryptographic techniques, developed for stronger systems, can impose a heavy computational burden. This limits the efficacy of blockchain applications by impeding their scalability and performance. The problem with the current approach is that it uses very computationally intensive cryptographic processes, which might be a bottleneck for devices with less power and memory. By offering cryptographic methods tailored to reduce computing cost, lightweight cryptography provides a more efficient option. Our suggested solution focuses on incorporating lightweight cryptography into blockchain in order to circumvent this obstacle. To drastically cut down on the blockchain system's resource consumption, our suggested approach makes use of lightweight cryptographic primitives. This allows the system to be deployed and operated successfully even in contexts with limited resources, while also improving its overall efficiency. Blockchain technology offers public digital ledgers and decentralised security, however it isn't ideal for devices with limited resources because of its high energy consumption, processing overhead, and significant delays.

Keywords: *Blockchain Technology , Lightweight Cryptography ,Resource-Constrained Environments ,Internet of Things (IoT) , Decentralized Security , Computational Overhead*

Introduction

When it comes to increasing the security, auditability, anonymity, and dependability of devices with limited resources, blockchain has recently garnered a lot of interest. The Internet of Things (IoT) is the third most important development in the information business, behind the fast-growing computer and internet sectors. In 2025, there will be more than 80 billion smart and low-constraint gadgets linked to the internet. The Internet of Things (IoT) overcomes the aforementioned evolutionary need of blockchain technology by effortlessly connecting heterogeneous objects with multiple networks that are centred on humans and machines. Blockchain was first introduced to the public in October 2008 by Nakamoto [1] in the cryptocurrency Bitcoin, which sought to create decentralised, peer-to-peer payment systems. Bitcoin offered a novel approach to the age-old problem of relying on other people's word in financial dealings[1][2]. Blockchain, with its unique trust-based mechanism, has created a major avenue for the thorough integration of technology and vertical industries. In order to facilitate better growth, the blockchain mechanism is supporting the integration of the real economy via strategic policies, technical developments, and market penetration. Data may be shared and stored in a distributed way using blockchain, which is a distributed ledger of blocks with an auditable, unchangeable timestamp. Cryptographic hashes of previous blocks are linked in a blockchain network, and the ledger comprises transaction data saved on every dispersed network node[3]. Personal information, contracts, medical records, and financial data (e.g., bitcoin, Ethereum) may all be kept. All nodes in a blockchain network contribute to a distributed ledger that records transactions. There is no longer a need for a central authority since other nodes in the network check and confirm new transactions[4]. The network's miners are the specific nodes responsible for retrieving fresh transactions from the memo pool. A new block is added to the blockchain network when the size of the current block surpasses a certain threshold; this process is called mining. Each miner adds new transactions into a block. A variety of consensus mechanisms, including PoW, PoS, PoA, PBFT, and many more, are used by the distributed ledger to facilitate mining[5].

A general blockchain network consists of transactions, blocks, block version, nonce, difficulty, previous hash value, timestamp, Merkle tree root hash, nodes, consensus, mining, and genesis block[6].

[1]*Assistant Professor, Computer Engineering Department, Government Engineering College, Modasa, nilesh.goriya@gecmodasa.ac.in*
[2]*Assistant Professor, Computer Engineering Department, Government Engineering College, Modasa, viral.patel@gecmodasa.ac.in*
[3]*Assistant Professor, Computer Engineering Department, Government Engineering College, Modasa, upendra.bhoi@gecmodasa.ac.in*
[4]*Assistant Professor, Computer Engineering Department, Government Engineering College, Modasa, nainesh.nagekar@gecmodasa.ac.in*

Transactions: A task that changes the state of the blockchain ledger. The transaction may involve the execution of a smart contract or the transfer of any valuable asset, depending on the application of blockchain

Blocks: A block in a blockchain comprises a block header and a block body. The header holds essential metadata about the block, including details like the block version, the timestamp, the hash of the previous block, and the Merkle tree root hash. The block body consists of data/information that is a set of valid transactions.

Block version: Block version indicates the version or format of the block's data structure and rules that should be applied when interpreting and processing the block by the blockchain network. The block version field is a way to communicate to network participants and software clients which set of rules or protocol versions should be used to handle the data within a particular block[7].

Nonce: Nonce is a variable that is used to change the output of the header hash. It is used to prove that a miner has completed a task along with the difficulty level. The miner will iterate the nonce until the header hash meets the necessary requirements if the difficulty requires that it begin with a consecutive series of four zeros[8][9]. The miner nodes will only compute the header hash once upon receiving the new block to verify the validity of the nonce.

Difficulty: Difficulty is defined as a parameter used in the PoW consensus algorithm to regulate the mining process. The difficulty level plays a critical role in maintaining the security and stability of the blockchain network.

Lightweight Cryptography

For applications with a tight budget or time crunch, lightweight cryptographic primitives are the way to go. The list of possible uses is long and includes things like wireless sensor networks, smartcards, the IoT, RFID, wireless body area networks, healthcare devices, and many more. A high degree of security is usually required since apps communicate personal and private data. There are a number of restrictions on the speed, memory, power, and energy consumption of these devices. These restrictions make it difficult to use conventional cryptography on devices with limited storage capacity[10]. Thus, encryption that is both lightweight and secure was developed. The exponential growth of new pervasive technologies gave rise to lightweight cryptography, a contemporary cryptographic method. Due to their expensive and complicated mathematical computation, classical cryptographic approaches provide a performance challenge when implemented in devices with limited resources. Massive amounts of RAM and computing power are required for these procedures. For devices with limited resources, classical cryptography might be costly to implement. Traditional cryptographic algorithms have been the subject of much effort to reduce their computing cost, speed, power consumption, and execution time [8][9][10]. On the other hand, the rising hardware needs have driven up the total operational expenses of this activity[11]. As shown in Figure 1, the size is the most critical aspect in deciding whether the implementation is feasible in devices with minimal constraints.

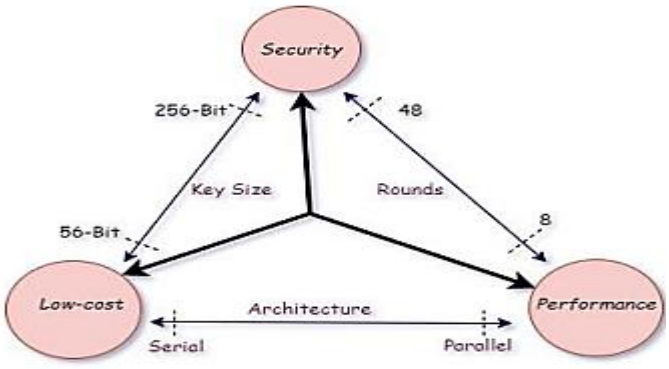

Fig 1: Parameters of Lightweight Cryptography

Energy harvesting gadgets and radio frequency identification (RFID) systems rely heavily on electricity. Power consumption is an important factor to consider for devices that run on batteries. Vibration sensors and cameras, which transmit large amounts of data, need a high throughput. On the other hand, systems that work in real-time, such as vehicle control, need very little latency for control processing[11][12]. Size is a measure of the efficiency and power of the encryption technique since power dependence is strongly related to hardware, which includes the size of the circuit or CPU in use. The importance of these calculations in determining efficiency has grown in recent years due to the fact that processing speed is impacted by power usage. However,

parallel processing skills are crucial to throughput. Lightweight cryptography seeks to reduce the total implementation cost of cryptographic primitives in terms of both software and hardware-oriented metrics like cycle rate, key size, power consumption, throughput, and Gate Equivalence (GE) [11], which measures area. Applications that rely heavily on smart and limited-resource devices should use lightweight cryptography[13].

Need For Lightweight Cryptography in the Blockchain Protocol

Lightweight cryptography is a subfield of cryptography that aims to minimise computational memory and energy consumption while yet delivering good security. Developing secure cryptographic algorithms and protocols that can run effectively on resource-constrained devices is the main focus of lightweight cryptography. These devices include embedded systems, mobile devices, and low-power Internet of Things (IoT) devices. After its inception, blockchain technology provided a decentralised and secure platform for smart contracts, data storage, and transactions; this led to its revolutionization in several sectors. Ensuring the integrity, secrecy, and validity of data on the network is the primary responsibility of blockchain's underlying security measures, especially cryptographic algorithms. Scalability and efficiency are of the utmost importance due to the increasing number of blockchain applications in many industries, including banking and supply chain management[14].

Because of this, lightweight cryptography is being reevaluated as an essential tool for dealing with these threats. The foundation of blockchain technology is the use of cryptographic primitives, which allow for the creation of an immutable ledger[15]. Blockchain networks aren't good for situations with limited resources or apps that need to execute transactions quickly because of these restrictions, which make them inefficient and slow.

In this context, lightweight cryptography is useful. Aiming to minimise computing needs, memory use, and energy consumption while providing good security assurances is the goal of lightweight cryptography. Yet, there are special considerations to bear in mind when incorporating lightweight cryptography into blockchain protocols in order to strike a balance between efficiency and security[16]. Find out if lightweight cryptographic algorithms are secure and whether they are good fits for blockchain applications. Assess their robustness against typical cryptographic attacks and blockchain-related issues. Improve the performance of blockchain networks using lightweight cryptography. Consider the memory and processing savings that resulted from using lightweight cryptographic primitives[17].

Determine how blockchain scalability is affected by lightweight cryptography. Look at how simple cryptographic techniques may ease the load on network nodes and speed up transaction processing. Smart metres, traffic sensors, and surveillance cameras are just a few examples of the resource-constrained devices used in smart cities. By using blockchain technology with lightweight cryptography, this data can be securely stored, preserving its integrity and confidentiality while minimising the utilisation of resources. Efficient product tracing and tracking is made possible by the lightweight encryption in blockchain. Authenticity, reduced fraud, and the prevention of counterfeiting may all be achieved via this. To protect users' privacy and confidentiality, blockchain-based messaging and communication systems may use lightweight cryptographic approaches[18].

Custom implementations are often necessary for lightweight cryptography, although they may be complicated and prone to errors. There is a higher chance of implementation weaknesses, which might lead to security breaches, when cryptographic operations are implemented using proprietary code. Sensors with insufficient processing power are a common component of resource-constrained devices. Because of the reduction in computing complexity, a lightweight method gives up some security in comparison to typical heavy cryptographic algorithms. On the other hand, blockchain technology's consensus methods make it resource-intensive[19]. The threat to data security grows in a resource-constrained setting in proportion to the number of networked devices. Therefore, it becomes a difficult undertaking to adapt blockchain to the environment with limited resources[20].

Problem Statement

There is a huge need for storage space, a lot of energy, and a lot of processing power for traditional blockchain technology. Because of this, devices like IoT and edge computing nodes, which have limited resources, may have trouble participating in the network efficiently..

• Conventional blockchains, such as Ethereum and Bitcoin, rely on consensus algorithms like PoW and PoS, which may be time-consuming and demanding on system resources. Therefore, congestion and expensive transaction fees are common outcomes for devices with restricted resources because of their low transaction throughput.

• Keeping the excitement around blockchain, which has become a widely used technology across many areas, presents a significant security problem. assaults

including 51% assaults, double spending, selfish mining, Sybil, and side-channel are consolidated here. Additional typical blockchain network attacks are also included.

Objectives

Help create blockchain systems that are both practical and strong, able to run well even on devices with little processing power.

1. Develop a strong cryptographic framework for lightweight blockchains that incorporates hash functions for data integrity verification, a consensus method that is efficient with resources, and lightweight cryptographic approaches.
2. Using effective protocols, a lightweight consensus mechanism, and quantum-resistant cryptographic protocols, provide a safe user initialization procedure while keeping communication channels lightweight.
3. Construct and deploy efficient verification procedures and consensus algorithms for the blockchain system to address 51% assaults and double-spend.
4. To regulate data transfer across networks, we suggest a new, lightweight design based on cryptographic hash functions.

Lightweight Blockchain Approach

Numerous kinds of smart, resource-constrained Internet of Things (IoT) sensors have found their way into people's everyday lives in recent years, along with numerous other novel technologies such as the Internet of Things (IoT), edge computing, cloud computing, and mobile computing. These Internet of Things devices can communicate with distant and edge servers, share data, and carry out a wide range of other tasks despite their low resource capabilities. However, due to operating in an atmosphere of mutual mistrust, these machines with limited resources are unable to fully cooperate, drastically reducing their efficiency on the task. As we've seen, blockchain technology is a great way to address concerns about privacy and security in the context of low-resource device applications. Unfortunately, their limited computing power, storage, and internet resources prevent them from meeting the cost of the blockchain consensus method and ledger storage[7][9]. Consequently, a lightweight blockchain is created for devices with limited resources, and several academics look at ways to make blockchain consensus algorithms run more efficiently with less computing power. Blockchain makes use of a number of consensus techniques, including ButFirst, Proof-of-Stake, Directed Acyclic Graph, Proof-of-Work, and Practical Byzantine Fault Tolerance. In this chapter, we build a lightweight blockchain using the idea based on the PoW consensus method. The Bitcoin system [1] has shown for years that PoW is the most secure consensus method, hence this is the purpose. Double-spend attacks may occur on DaG-based blockchains; PBFTs have poor scalability and latency; the Mathew effect, which makes the wealthy become wealthier, can affect PoSs; and spam and denial-of-service assaults are real concerns. Blockchain players (miners) compete to solve cryptographic puzzles—difficult to solve but easy to validate—as part of the PoW consensus process. The blockchain network will award the winner and provide them the ability to build a new block.

Internet of Things devices cannot directly connect the blockchain framework due to PoW's excessive processing power requirements. When it comes to the blockchain platform, security is a top priority. The amount of transactions will increase as more Internet of Things devices join a blockchain network that is more secure. A fixed transaction fee is applied to all blockchain transactions. Therefore, the integrity of the blockchain network is highly related to its usefulness. There would be more advantages to the platform if it is safe. The security of a blockchain with a PoW consensus mechanism is solely dictated by the network's aggregate processing power. Bitcoin is a method that uses distributed time-stamping services to digitally sign transactions with hashes, rather than depending on the idea of proof-of-work (PoW), which requires a trusted third party. Bitcoin users run the risk of engaging in fraudulent transactions where they spend the same cryptocurrency twice since electronic data is easily replicable and there is no trustworthy third party that can confirm the expenditure of digital coins.

Methodology

This paper proposes a blockchain system that uses a lightweight hash function to improve the efficiency, security, and speed of the blockchain hash algorithm. When it comes to computational throughput, area, and energy consumption, lightweight hash functions like SPONGENT, LESAMNTA-LW, and PHOTON demonstrate better performance. The suggested design updates the hash function depending on the amount of transactions to ensure the blockchain network is available. Next, we linked all of the data blocks together using a flexible hash chain that we generated using these hash algorithms. By using this approach, processing load and delay may be decreased. Our simulation findings show that the suggested architecture works well in situations when data has to be processed in a certain amount of time and with limited resources, such as in the area of monitoring and supervision. By modifying the mining hashing algorithm, it is able to modify network traffic.

Lightweight consensus, secure communication channels using Quantum Key Distribution (QKD) protocols, and quantum resistant cryptographic protocols are all part of the work's new user initialization procedure. Data transfers are made safe and efficient with lower key sizes and better computing efficiency by using Lightweight Elliptic Curve safe Key Exchange and Authentication (LECSKEA). Direct meta-data storage, lightweight cryptographic methods, a resource-efficient consensus process (Harmonic ByzRaft-PoA Fusion), and the inclusion of hash functions for data integrity verification are all components of a robust lightweight blockchain security framework. Our method also optimises storage, introduces redundancy for fault tolerance, and efficiently distributes storage load across the network for resilient and resource-efficient storage infrastructure. It also implements Efficient Lightweight Storage Management in Blockchain through a carefully crafted scheme based on lightweight Reed-Solomon (LRS) erasure code. This comprehensive approach guarantees that blockchain implementation across many applications and contexts is secure, efficient, and adaptable.

The safety of the blockchain network is a top priority. Here we will go over two algorithms:

Reduces mining overhead latency using the "Distributed Execution Time_based Consensus Algorithm" (DETCA).

To prevent 51% attacks and double spending, use the "Randomised Node-selection Algorithm" (RNSA) to choose the verification node. The mining and verification processes in a conventional blockchain include every node in the network.

The processing and communication overhead it generates is substantial. Accordingly, not every node will participate in mining under the proposed scheme. After choosing a miner node from the mining table, the verification procedure uses a randomly generated series of nodes. The suggested architecture is shown in Figure 2.

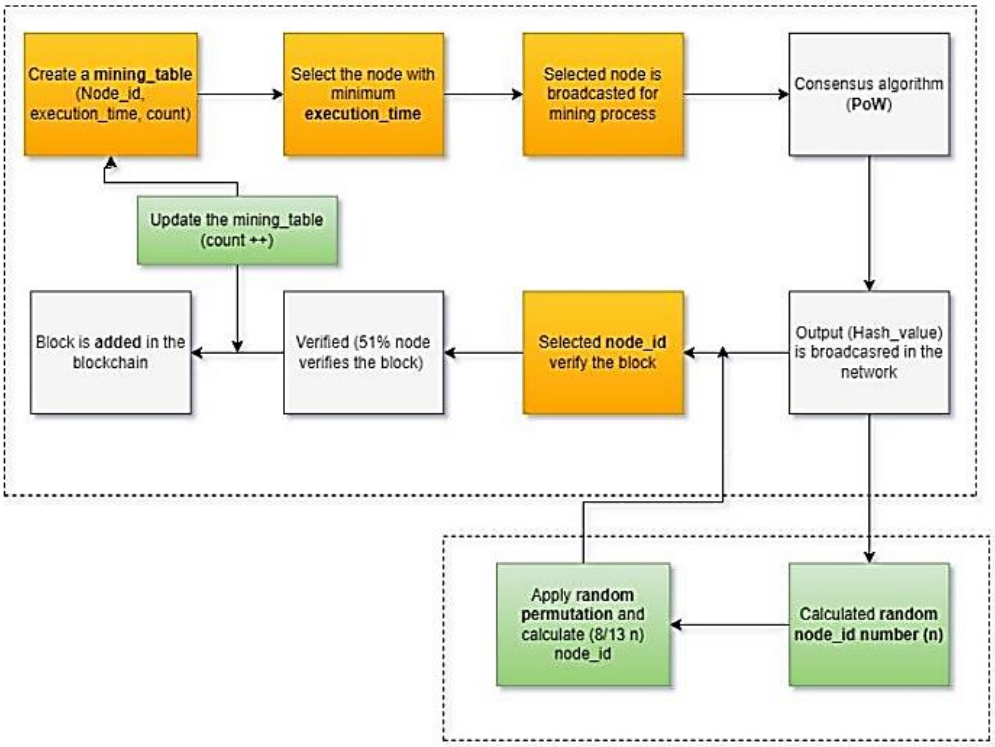

Fig 2. Flow Diagram of the Proposed Architecture(Source: T Eisenbarth Springer Book)

Proposed RNSA Algorithm

- The mining table and the consensus algorithm are the two main components of a block's mining operation. Every node in the network that may be considered a miner has its own database of mining results. The mining table is used to pick the node that will mine the block using the PoW consensus technique. Once chosen, the node is disseminated across the network. Node id, execution time, and count are the three parameters used by the source node to construct a mining table in algorithm 1. The mining table's procedures and results list. After selecting a miner node based on minimal count and execution time, the node is propagated across the network to begin mining. Once mining is complete, the count value in the mining table is increased to reflect the successful validation of the transaction by the

chosen miner node using the PoW consensus process. Three parameters are included in the mining table:

- Node_id: Node number
- The time it takes to process a block during mining is called execution time.
- The number of operations completed by each node is called count.

Figure 3 shows the results of sorting a table by count and execution time. N3 is chosen as a miner node to mine the block since it has the smallest count and execution time in this table. One is added to the block's total after mining. The next step in preventing hunger is sorting the database according to execution time and count.

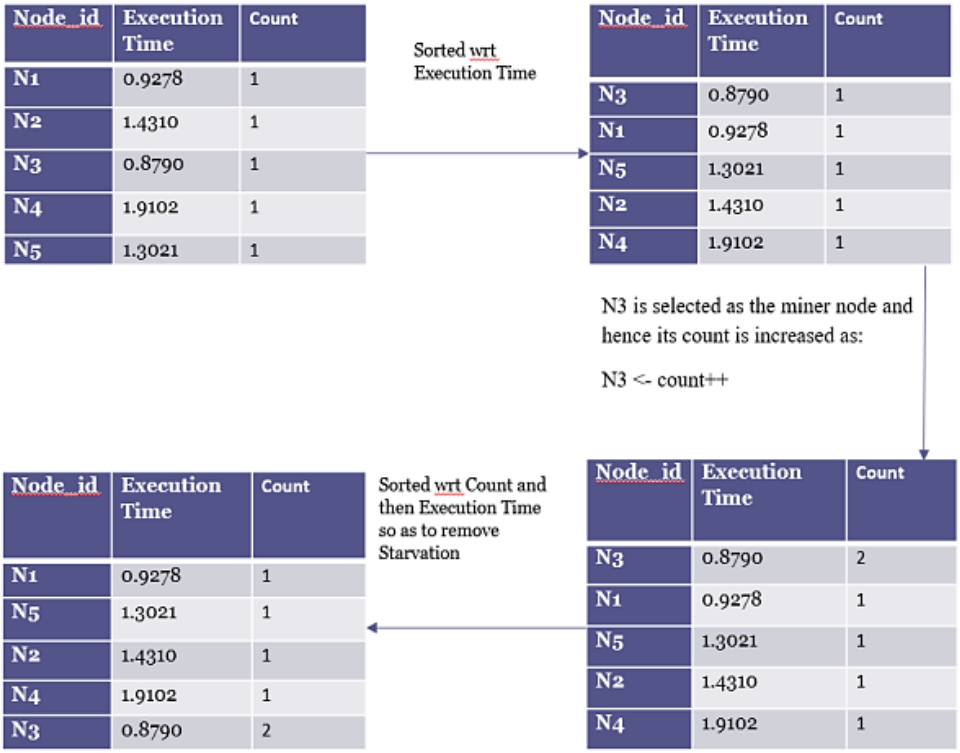

Fig 3: Mining table

Conclusion

An end-to-end secure blockchain architecture that is lightweight and optimised for the IoT context was therefore suggested in this study. Using its DETCA approach, the proposed work optimises CPU utilisation and lowers energy consumption. It also employs the RNSA algorithm to mitigate 51% assaults and double-spend. The suggested techniques reduced data theft likelihood, computational strain on networks, energy consumption, and mining time, according to the simulation findings. Positive outcomes include a considerable decrease in mining overhead, prevention of the double-spending issue, and protection against the 51% assault.

References

[1] 1.Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008).

[2] Kumar Saurabh and Ashutosh Saxena. “Blockchain Technology concepts and applications.” Book, Wiley Emerging Technology Series.

[3] Rolfes, Carsten, Axel Poschmann, Gregor Leander, and Christof Paar. "Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents." In Smart Card Research and Advanced Applications: 8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008. Proceedings 8, pp. 89-103. Springer Berlin Heidelberg, 2008.

[4] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54, no. 15 (2010): 2787-2805.

[5] Weis, Stephen A., Sanjay E. Sarma, Ronald L. Rivest, and Daniel W. Engels. "Security and privacy aspects of low-cost radio frequency identification systems." In Security in Pervasive Computing: First International Conference, Boppard, Germany, March 12-14, 2003. Revised Papers, pp. 201-212. Springer Berlin Heidelberg, 2004.

[6] Chen, Min, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor CM Leung. "Body area

networks: A survey." Mobile networks and applications 16 (2011): 171-193.

[7] Zhang, Guang He, Carmen Chung Yan Poon, and Yuan Ting Zhang. "A review on body area networks security for healthcare." International Scholarly Research Notices 2011 (2011).

[8] O'Melia, Sean, and Adam J. Elbirt. "Enhancing the performance of symmetric-key cryptography via instruction set extensions." IEEE transactions on very large scale integration (VLSI) systems 18, no. 11 (2009): 1505-1518.

[9] Elbirt, Adam J. "Fast and efficient implementation of AES via instruction set extensions." In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), vol. 1, pp. 396-403. IEEE, 2007.

[10] Constantin, Jeremy Hugues-Felix, Andreas Peter Burg, and Frank K. Gurkaynak. "Investigating the potential of custom instruction set extensions for SHA-3 candidates on a 16-bit microcontroller architecture." (2012).

[11] Martín, Honorio, Pedro Peris-Lopez, Juan E. Tapiador, and Enrique San Millán. "An estimator for the ASIC footprint area of lightweight cryptographic algorithms." IEEE Transactions on Industrial Informatics 10, no. 2 (2013): 1216-1225.

[12] Law, Yee Wei, Jeroen Doumen, and Pieter Hartel. "Survey and benchmark of block ciphers for wireless sensor networks." ACM Transactions on Sensor Networks (TOSN) 2, no. 1 (2006): 65-93.

[13] Biryukov, Alex, and Leo Perrin. "State of the art in lightweight symmetric cryptography." Cryptology ePrint Archive (2017).

[14] Batina, Lejla, Amitabh Das, Barış Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, and Tolga Yalçın. "Dietary recommendations for lightweight block ciphers: power, energy and area analysis of recently developed architectures." In Radio Frequency Identification: Security and Privacy Issues 9th International Workshop, RFIDsec 2013, Graz, Austria, July 9-11, 2013, Revised Selected Papers 9, pp. 103-112. Springer Berlin Heidelberg, 2013.

[15] Ågren, Martin. "On some symmetric lightweight cryptographic designs." (2012).

[16] Mahmood, Khalid, Shehzad Ashraf Chaudhry, Husnain Naqvi, Saru Kumari, Xiong Li, and Arun Kumar Sangaiah. "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication." Future Generation Computer Systems 81 (2018): 557-565.

[17] Odlyzko, Andrew M. "Discrete logarithms in finite fields and their cryptographic significance." In Workshop on the Theory and Application of of Cryptographic Techniques, pp. 224-314. Berlin, Heidelberg: Springer Berlin Heidelberg, 1984.

[18] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21, no. 2 (1978): 120-126.

[19] Chien, Hung-Yu, and Chi-Sung Laih. "ECC-based lightweight authentication protocol with untraceability for low-cost RFID." Journal of parallel and distributed computing 69, no. 10 (2009): 848-853.

[20] Dutta, Indira Kalyan, Bhaskar Ghosh, and Magdy Bayoumi. "Lightweight cryptography for internet of insecure things: A survey." In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0475-0481. IEEE, 2019.