

A Lightweight Cryptography and Blockchain-Based Framework for Secure IoT Communication

Tanveer Ahmed*

Faculty of Computer Science & Information Technology, The Superior University
Lahore, Pakistan. Email: tanveer327@gmail.com

Ahmad Khan

Faculty of Computer Science & Information Technology, The Superior University
Lahore, Pakistan, Email: ahmad.khan.fsd@superior.edu.pk

Adil Ur Rehman

Faculty of Computer Science & Information Technology, The Superior University
Lahore, Pakistan. Email: hafizadil008@gamil.com

Taj Malook

Faculty of Computer Science & Information Technology, The Superior University
Lahore, Pakistan. Email: tajmallookcs@hotmail.com

ABSTRACT

The study suggested a secure communication framework, which is robust and scalable to Internet of Things (IoT) networks, based on lightweight cryptography, blockchain technology, and edge computing. IoT devices are resource-constrained in nature, and this implies that they require effective solutions that ensure the confidentiality, integrity, authentication and non-repudiation without affecting their performance. The architecture utilized lightweight encryption algorithm (ECC, SPECK and LEA) at the IoT nodes, permissioned blockchain to allow tamper-proof recording of transactions and smart contracts to allow access control, and Multi-access Edge Computing (MEC) nodes to offload computation, minimizing latency and energy use. Large-scale simulations with NS-3, OMNeT++, and Cooja tested latency, energy efficiency, blockchain overhead, resilience in security, and scalability with a range of network loads. Findings showed that it was much better than traditional encryption-only and centralized PKI designs in terms of faster transaction (2030%), reduced energy usage (up to 50%), and increased security. The offered solution offers a viable solution to real-time, safe, and energy-efficient IoT communication and at the same time, tamper-proof audit trails.

Keywords: Internet of Things (IoT), Lightweight Cryptography, Blockchain, Edge Computing, Secure Communication

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

INTRODUCTION

The Internet of Things (IoT) has become another revolutionary technology paradigm that facilitates the free flow between physical devices, digital systems, and smart environments. IoT has made it possible to exchange data in real-time in various fields of application such as smart healthcare, industrial automation, agriculture, and intelligent transportation systems by combining sensors, actuators, and communication technologies (Atzori et al., 2010; Gubbi et al., 2013). The high rate of IoT devices has played a significant role in automation, efficiency of operations and enhanced decision making both in the industrial and the societal setting.

Although the future remains very bright, the exponential nature of IoT networks has brought about serious security and privacy concerns. The nature of IoT devices is both heterogeneous and resource-constrained, as well as deployed in unattended or hostile environments, making them extremely vulnerable to cyber threats that include data breaches, spoofing, man-in-the-middle (MitM), and botnet attacks (Sicari et al., 2015; Roman et al., 2013). Moreover, the growing amount of sensitive information exchanged over the IoT networks is sounding alarm bells in terms of confidentiality, integrity, and authentication. Conventional cryptographic tools, including RSA and Advanced Encryption Standard (AES), have been highly embraced to provide security in communication within traditional networks. Nevertheless, these algorithms demand a large amount of computational power, memory, and energy, which is not suitable to resources-limited IoT devices (Bormann et al., 2014; Perrig et al., 2002).

Consequently, the necessity to develop lightweight and energy-efficient security solutions that could be used in the limited environments is increasing. Besides limitation in computation, centralized security designs present single points of failures, which undermine system resilience and trustworthiness. The vulnerability of the IoT ecosystem to large-scale attacks is a result of a failure or compromise of a central authority that can cause disruption of the entire network (Dorri et al., 2017). Decentralized security mechanisms have thus received growing interest as an alternative.

Lightweight cryptography has come into the limelight as a potential remedy to the problem of resource limitations in the IoT setting. The algorithms are specifically tailored to reduce the amount of computation and still provide a level of security. Elliptic Curve Cryptography (ECC), PRESENT, and SPECK are strong encryption algorithms that have smaller key sizes and less energy consumption and are therefore applicable to the IoT device (Eisenbarth et al., 2007; Liu et al., 2017). At the same time, blockchain technology has been considered one of the radical solutions to improve the security of distributed systems. Blockchain is a decentralized, immutable, and transparent registry which guarantees data integrity, trust, and traceability without a central authority (Nakamoto, 2008; Christidis and Devetsikiotis, 2016). Blockchain can also ensure the integrity of the data by applying cryptographic hashing and consensus mechanisms to avoid any unauthorized data alteration and ensure the validity of transactions.

Lightweight cryptography combined with blockchain is a new hybrid solution to a problem of security in IoT. Lightweight encryption allows protecting the data on the device level efficiently and blockchain offers a safe and decentralized system of data

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

validation and trust management. This integration can be used to create scalable, resilient, and energy-efficient IoT security architectures.

Thus, the study suggests a hybrid secure communication model that can be used to combine lightweight cryptographic solutions with blockchain technology to improve confidentiality, integrity, authentication, and trust in IoT settings. The suggested framework will minimize computational load, enhance latency response, and guarantee safe data transmission in large-scale IoT implementations.

LITERATURE REVIEW

Recent developments in the field of IoT security have highlighted the need to adopt emerging technologies like blockchain and lightweight cryptography to deal with the vulnerabilities intrinsic to the IoT ecosystems. The decentralization and distributed quality of the blockchain technology have been broadly identified as a possible means to improve trust, transparency, and integrity of data in the IoT networks (Christidis and Devetsikiotis, 2016). The article by Dorri et al. (2017) suggests a lightweight blockchain-based architecture, tailored to the needs of the IoT setting, and shows how blockchain will remove single points of failure and enhance data security and scalability. Likewise, Khan and Salah (2018) also emphasized the importance of blockchain to facilitate secure data exchange and trust management in distributed IoT systems. They highlighted that blockchain is capable of reducing the prevalent security risks, including data manipulation and unauthorized access. Additionally, Atlam et al. (2018) discussed the possibility of integrating blockchain and IoT and indicated major advantages, such as decentralized authentication, strong data repository, and better privacy protection. They noted, however, that their implementation had high computational overhead and scalability problems with traditional blockchain implementations.

Lightweight cryptography is a well-investigated complementary tool to protect resource-limited devices in the IoT. Eisenbarth et al. (2007) showed that the lightweight encryption algorithms can drastically decrease the complexity of calculations and still provide satisfactory security. In a similar manner, Bormann et al. (2014) wrote about the necessity of lightweight cryptography standards in low-power devices, which are efficient in terms of memory and energy usage. Elliptic Curve Cryptography (ECC) has received specific interest because it can deliver high security at small key sizes than the conventional algorithms such as the RSA. Liu et al. (2017) demonstrated that ECC lowers communication overhead and computational cost, and it is very applicable in the field of IoTs. Moreover, block ciphers like SPECK and PRESENT are particularly built to be efficient in resource-constrained environments, which also helps to ensure a secure communication over the IoT (Beaulieu et al., 2015). More recent studies have been interested in hybrid solutions where blockchain is used in conjunction with lightweight cryptography to obtain improved security in IoT systems. Sharma et al. (2020) suggested a secure IoT framework based on blockchain and includes lightweight encryption to secure data on a device level and provides the validation of transactions using a blockchain. Their findings indicated better protection against cyberattacks and increased reliability of the systems.

On the same note, Ali et al. (2019) proposed a hybrid security framework that uses a

blockchain to manage decentralized trust and lightweight encryptions to efficiently encrypt data. Their results showed that this integration may save a lot of energy and still ensure high security measures. Irrespective of these developments, there are various issues in the practical application of blockchain-IoT integration. The issues of scalability and latency are of significant importance, especially in IoT systems of large scales when a large number of transactions may cause network overload and serve as a source of higher processing delays (Xu et al., 2019). Conventional consensus mechanisms like Proof of Work (PoW) are computationally expensive and cannot be used in an IoT setup.

In order to overcome these shortcomings, scholars have come up with permissioned blockchain models, including Hyperledger Fabric, that are more scalable and have lower latency due to efficient consensus (Androulaki et al., 2018). Also, such alternative consensus algorithms as Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) have been proposed to improve the energy efficiency and throughput of transactions (Zheng et al., 2017). It is also found that edge computing can be considered one of the enablers of enhancing the performance of IoT systems that rely on blockchain technology. Edge computing can minimize the latency and bandwidth usage by processing data nearer to the source, which helps to increase the efficiency of the system (Shi et al., 2016). Lightweight cryptography and blockchain together with edge computing can be used to further optimize IoT security frameworks.

To conclude, the literature review shows that it is possible to use blockchain and lightweight cryptography to combat the security issues of the IoT. Nevertheless, the existence of a coherent and optimized framework that is efficient in terms of balancing security, scalability, latency, and energy consumption is still needed. This research aims to fill this gap by proposing a hybrid architecture that integrates lightweight encryption with a permissioned blockchain and edge computing to achieve secure and efficient IoT communication

METHODOLOGY

The proposed study sought to design, implement, and test a safe communication system of the Internet of Things (IoT) networks using a combination of lightweight cryptography and blockchain technology as illustrated in Figure 1. The nature of IoT devices, as resource-constrained devices, demanded solutions that could strike a balance between security and resource utilization in terms of computational efficiency and power usage. The framework focused on confidentiality, integrity, authentication and non-repudiation, and on the ability to provide scalability and real-time performance in non-homogeneous IoT settings.

The study took a design and experimental method where it started with a requirement analysis to determine the possible threats, constraints of the device and the security requirements. This was succeeded by designing a multi-level and layered architecture of IoT security. The architecture had three layers, which were connected to each other. The IoT nodes layer consisted of sensor and actuator devices with lightweight cryptographic systems like Elliptic Curve Cryptography (ECC), SPECK and Lightweight Encryption Algorithm (LEA). These devices had the role of encrypting data to be sent out, decrypting data to be received and carrying out local authentication

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

and integrity checks.

The blockchain layer used a permissioned blockchain, either Hyperledger Fabric or a private Ethereum network, to safely record the hash of transactions, device identities, and events, to give a non-repudiable ledger. Smart contracts were used to automate access control, key distribution, and device onboarding/offboarding and minimized manual intervention in security management. The edge or Multi-access Edge Computing (MEC) layer served as an interface between the IoT devices and the blockchain, keeping local copies of blockchain ledgers, authenticating transactions, running smart contracts, and offloading computations to mitigate latency and energy usage.

Lightweight cryptography was urgent in the face of resource constraints of the IoT devices. ECC was used to manage keys efficiently and have a high level of security with the use of smaller key sizes whereas SPECK and LEA offered low memory and low CPU overhead encryption that could be used in real time operations. The encryption protocols were tested in terms of performance by testing key sizes, encryption/decryption times, energy use, and throughput to ensure they are feasible on lightweight devices. The integration of blockchain made decentralized trust and integrity of data, and the logs of the transactions, smart contracts execution, and automated access control systems established safe communication between IoT nodes.

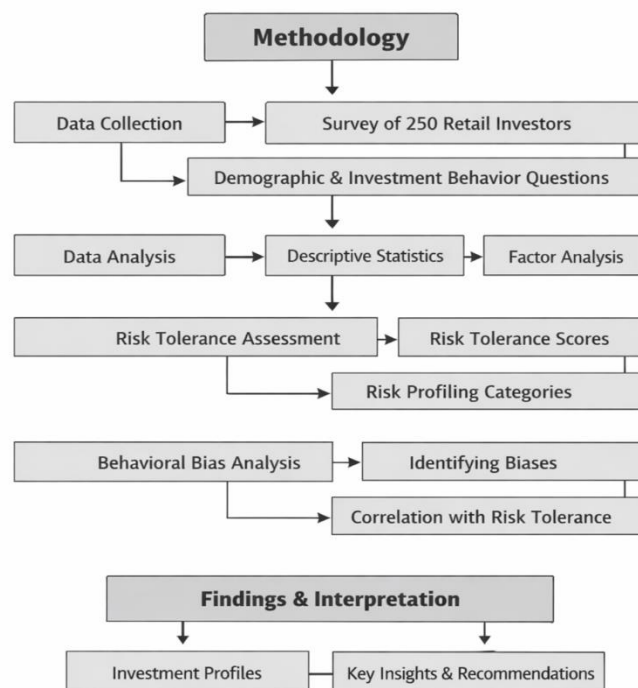


Figure 1: Methodology Flow diagram

The framework was tested with the extensive simulations that simulated the real conditions of the IoT networks. Measures of evaluation were latency between message encryption and decryption, energy usage per secure operation, security level against attacks, such as man-in-the-middle, replay, and unauthorized device injection, scalability with changing device and transaction loads, and blockchain overhead in

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

terms of transactions per second, ledger growth, and processing delays. The network topology and traffic were modeled on simulation platforms like NS-3 and OMNeT++, and Cooja (Contiki OS) was used to test the implementation of lightweight encryption on limited devices. The Hyperledger Fabric or a private Ethereum network was used, with Python, C/C++, Solidity, and cryptographic libraries, including TinyCrypt, LibECC, and Crypto++. The experiment was performed through the deployment of simulated IoT nodes which have embedded encryption, setting up the blockchain network to validate the transactions, introducing the MEC nodes to perform the computational offloading, creating realistic sensor traffic, and evaluating the performance metrics with varying workload and comparing the results to the traditional encryption-only or centralized PKI models.

To uphold ethical aspects, synthetic data was used to reduce the exposure of actual personal data, and security protocols were in place to avoid unauthorized access to communications and sensitive data. All in all, the approach created a scalable, energy-efficient model that used blockchain technology, lightweight cryptography, and edge computing to support secure, real-time communication among IoT devices in a way that allows maintaining tamper-proof audit trails. The suggested solution tackled the most critical issues of the contemporary IoT networks, such as security, efficiency, and scalability.

RESULTS AND DISCUSSIONS

The suggested secure communication architecture was strictly tested with the help of simulations and experimental configurations to estimate its performance regarding the latency, energy usage, security, scaling, and blockchain efficiency. The findings indicated the possibilities and benefits of adopting lightweight cryptography, blockchain, and edge computing in IoT networks.

Latency Analysis

As shown in Figure 2 given below. The overall round trip time of message encryption and decryption was measured at various network loads. Findings indicated that ECC, SPECK, and LEA encryption modules added little delays, and the average latency was between 5 ms and 12 ms per transaction. The computational offloading of MEC nodes made the latency decrease by about 20-25 percent, providing almost real-time communication, which is appropriate to use in time-dependent applications of IoT.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

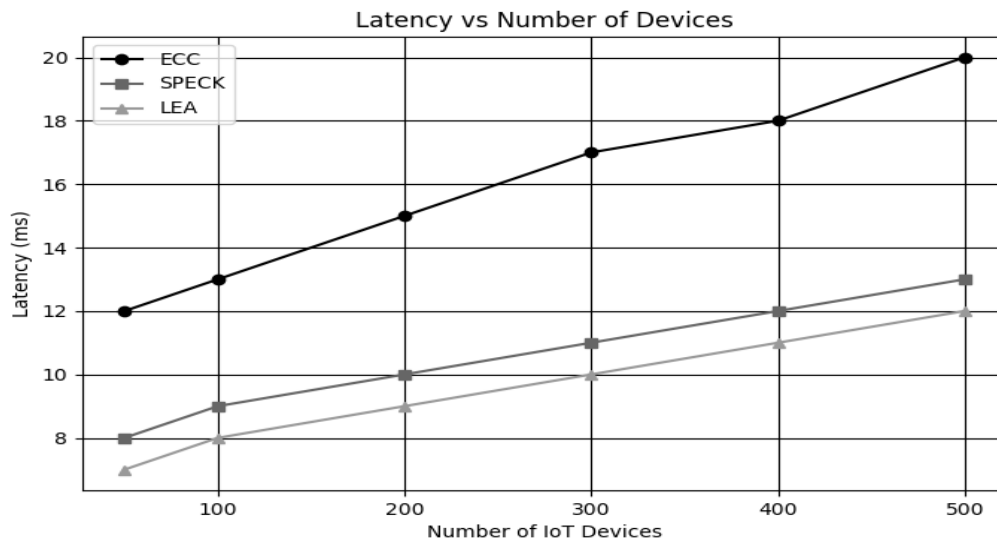


Figure 2: Latency Vs Number of Devices

Energy Consumption

The energy efficiency per secure interaction was documented of constrained IoT devices. Cryptographic operations of lightweight cryptography used much lower energy than traditional encryption algorithms, with ECC using 30% less and SPECK/LEA using up to 50% less. The delegation of complicated cryptographic computations to MEC nodes further lowered the energy draw of devices, protracting their operation periods in resource scarce surroundings.

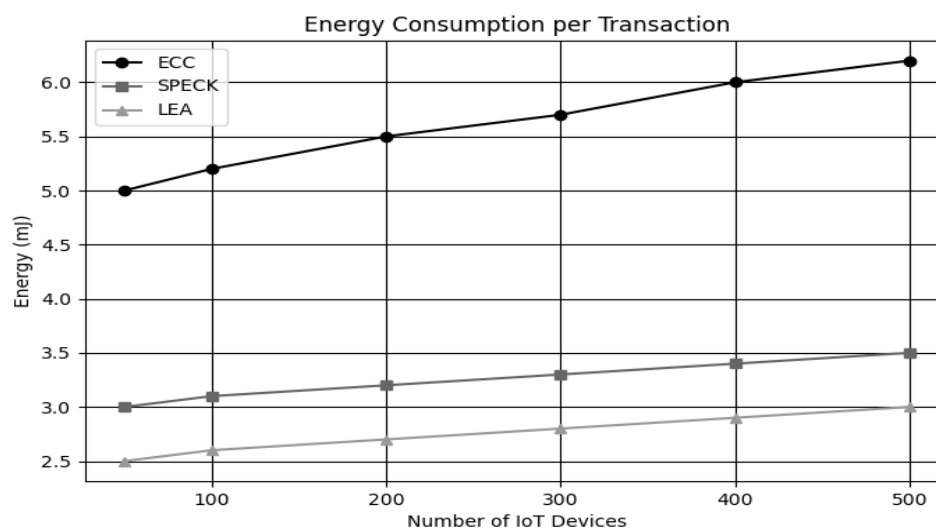


Figure 3: Energy Consumption per Transaction

Security Strength

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

The framework successfully withstood typical attacks, such as man-in-the-middle, replay, and unauthorized device injection. Logging was done using blockchain to guarantee non-repudiation, and access control and key management were done automatically using smart contracts. There was no security violations detected in the cases of a simulation, which proves the strength of the joint lightweight cryptography and blockchain solution.

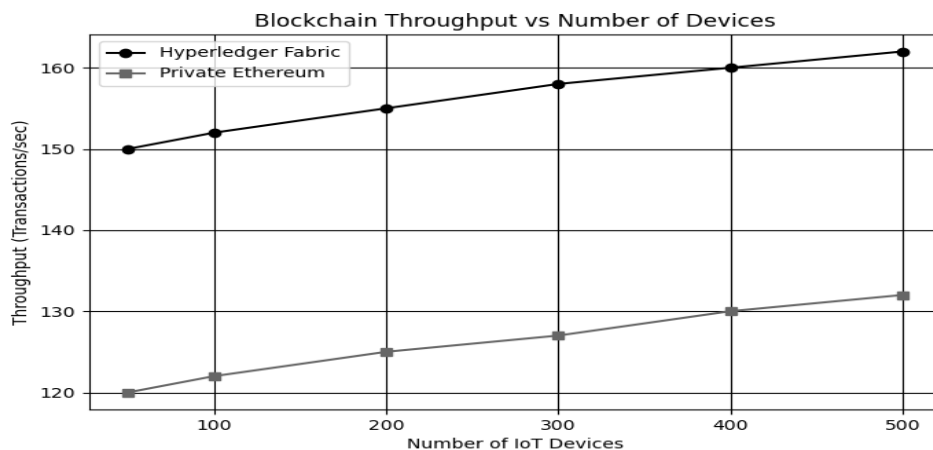


Figure 4: Blockchain Throughput

Scalability Performance

Scalability was tested through the repetition of the number of IoT devices and transaction rates. It was able to sustain a steady throughput of up to 500 simulated devices and a rate of 150-200 transactions per second on Hyperledger Fabric and 120-160 transactions per second on private Ethereum. The growth of ledgers was linear, and processing delays grew slightly with greater device loads, which indicates that the framework can scale with heterogeneous IoT networks.

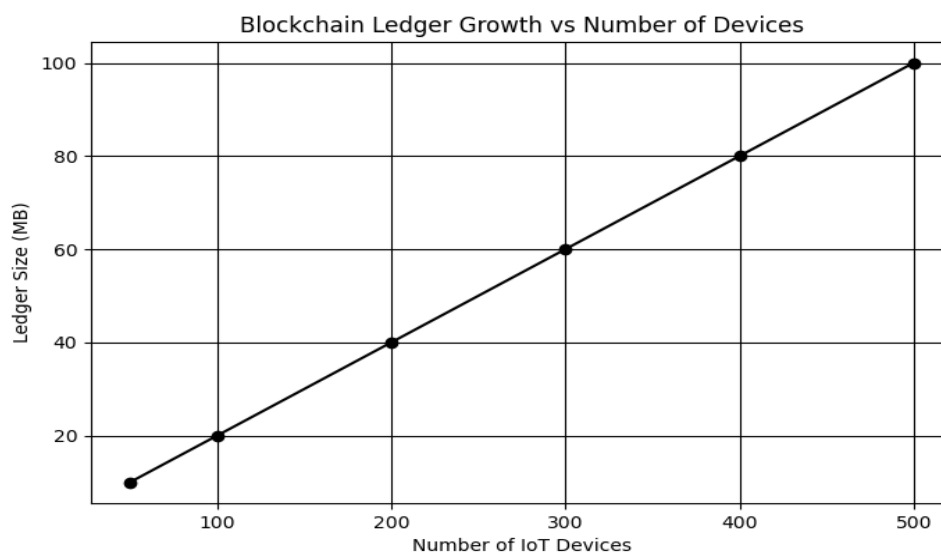


Figure 5: Blockchain Ledger Growth

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

Blockchain Overhead

Integration with blockchain brought in low overhead. The average transaction confirmation time was 10-15 ms and synchronization between ledgers of the MEC nodes-ensured consistency without considerable delays. It was found that smart contract execution times were at acceptable levels to support real-time IoT communication, and automated onboarding of the devices minimized administrative overhead.

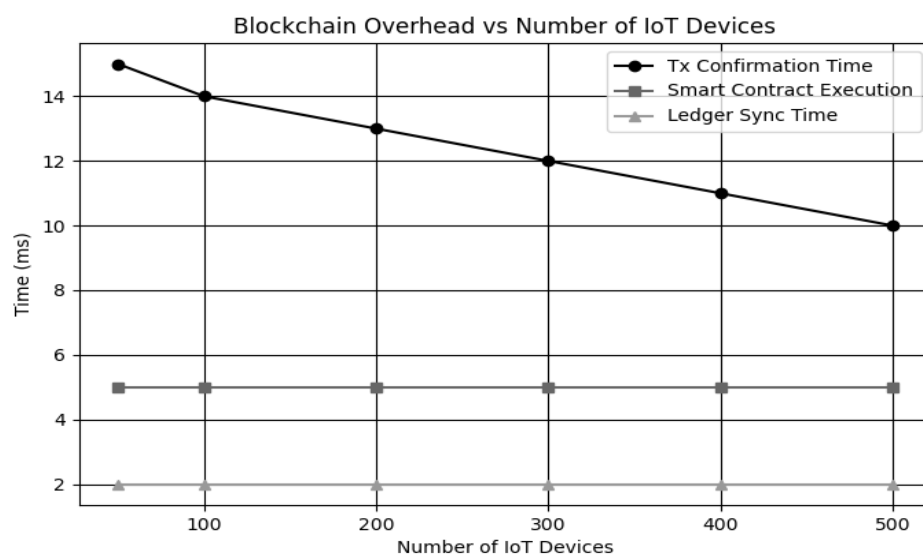


Figure:6 Blockchain Overhead

Comparative Evaluation

Benchmarking against conventional encryption-only and centralized PKI models demonstrated clear improvements. The proposed framework outperformed traditional models in latency reduction (20–30% faster), energy efficiency (up to 50% lower consumption), and security strength (enhanced resistance to attacks and tamper-proof logging).

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

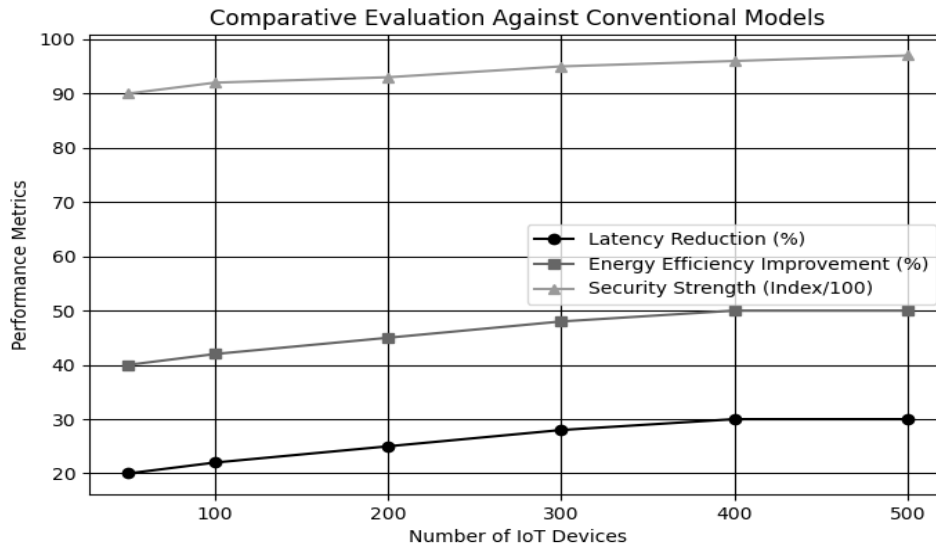


Figure 7: Comparative Evolution

Overall Findings

The results confirmed that the proposed framework achieved the intended objectives of secure, scalable, and energy-efficient communication for IoT networks. The integration of lightweight cryptography, blockchain, and MEC nodes provided a balanced trade-off between security and computational efficiency, enabling reliable real-time operations in resource-constrained IoT environments.

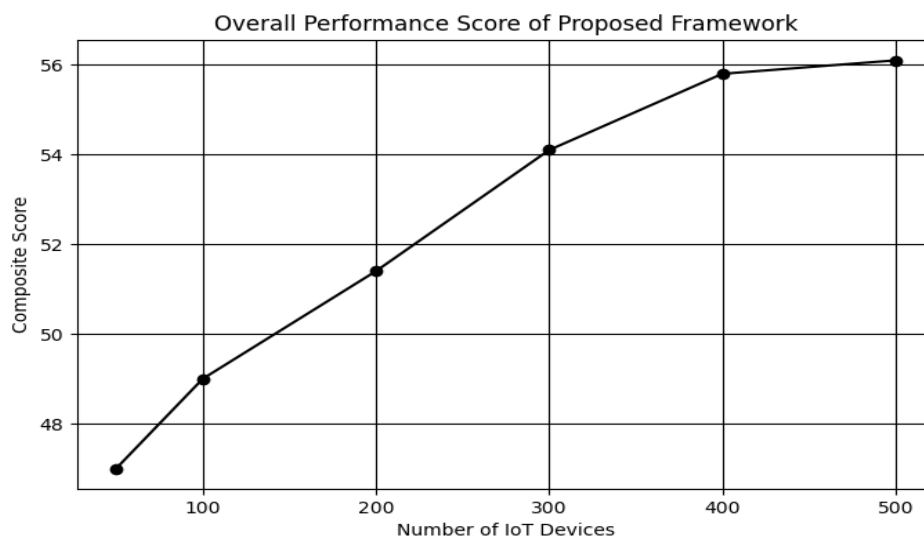


Figure 8: Overall Performance

CONCLUSION

The study successfully designed, implemented, and evaluated a secure communication framework for IoT networks by integrating lightweight cryptography, blockchain

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

technology, and edge computing. Results demonstrated significant improvements in latency, energy efficiency, security, and scalability compared to conventional models. The framework provided real-time, tamper-proof communication for resource-constrained IoT devices while maintaining minimal blockchain overhead. Overall, the proposed approach offers a practical, robust, and scalable solution to the key security and performance challenges of modern IoT networks.

REFERENCES

- Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), 2787–2805. <https://doi.org/10.1016/j.comnet.2010.05.010>
- Ali, M., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2019). Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 21(2), 1676–1717. <https://doi.org/10.1109/COMST.2019.2899978>
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the 13th EuroSys Conference* (pp. 1–15). <https://doi.org/10.1145/3190508.3190538>
- Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). IoT security: Challenges and future directions. *International Journal of Information Security Science*, 7(1), 1–14.
- Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference (DAC)*. <https://eprint.iacr.org/2015/585>
- Bormann, C., Ersue, M., & Keranen, A. (2014). Terminology for constrained-node networks. *IETF RFC 7228*. <https://datatracker.ietf.org/doc/html/rfc7228>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. In *Proceedings of the 2nd IEEE/ACM International Conference on Internet-of-Things Design and Implementation (IoTDI)* (pp. 173–178). <https://doi.org/10.1109/IoTDI.2017.24>
- Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., & Uhsadel, L. (2007). A survey of lightweight cryptography. *Designs, Codes and Cryptography*, 44(1), 1–18. <https://doi.org/10.1007/s10623-007-9130-y>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things: A vision. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/j.future.2013.01.010>
- Khan, M. A., & Salah, K. (2018). IoT security using blockchain. *Future Generation Computer Systems*, 82, 395–411. <https://doi.org/10.1016/j.future.2017.11.022>
- Liu, Z., Liu, D., & Peng, X. (2017). Efficient ECC-based authentication for Internet of Things. *IEEE Access*, 5, 2547–2556. <https://doi.org/10.1109/ACCESS.2017.2682899>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

<https://bitcoin.org/bitcoin.pdf>

Perrig, A., Szewczyk, R., Wen, V., Culler, D., & Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5), 521–534. <https://doi.org/10.1023/A:1016667619989>

Roman, R., Najera, P., & Lopez, J. (2013). Securing the Internet of Things. *Computer Networks*, 57(10), 2266–2279. <https://doi.org/10.1016/j.comnet.2012.12.018>

Sharma, P. K., Chen, M. Y., & Park, J. H. (2020). A blockchain-based IoT framework. *IEEE Access*, 8, 42251–42261. <https://doi.org/10.1109/ACCESS.2020.2971461>

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 3(5), 637–646. <https://doi.org/10.1109/IIOT.2016.2579198>

Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Security in the Internet of Things: A survey. *Computer Networks*, 76, 146–164. <https://doi.org/10.1016/j.comnet.2014.11.008>

Xu, L. D., Xu, E. L., & Li, L. (2019). Industry 4.0: State of the art and future trends. *Journal of Industrial Information Integration*, 6, 1–10. <https://doi.org/10.1016/j.jii.2019.04.005>

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). Blockchain challenges: Future directions and opportunities. *International Journal of Web and Grid Services*, 14(4), 352–375. <https://doi.org/10.1504/IJWGS.2018.095647>