Shodh Sari-An International Multidisciplinary Journal

2025, Vol. 04, Issue 02, 111-128
ISSN: 2959-1376
DOI: https://doi.org/10.59231/SARI7813

An Energy-Efficient Hybrid Security Model for Large-Scale Cloud Systems: Integrating Blockchain, Quantum Cryptography, and Post-Quantum Algorithms

A, Neethu V[1], Vaishnav, Arun[2] and Khan, Mohammad Akram[3]

[1]Research Scholar, Department of Computer Science Engineering & Technology, Madhav University, Sirohi, Rajasthan, India

[2]Assistant Professor, Faculty of Computing and Informatics, Sir Padampat Singhania University, Udaipur, Rajasthan, India.

[3]Assistant Professor, Department of Computer Science and Application, Madhav University, Sirohi, Rajasthan, India

Abstract

Cloud computing can be used to utilized to ensure data security and energy efficiency in large-scale environments. This paper, introduced in hybrid security model to integrate the block chain technology, Quantum Cryptography, and Post Quantum algorithms. This model provides a strong framework for ensuring data security and integrity. Post Quantum Cryptography algorithm might be utilized to discuss the prospects for cyber-attacks in quantum computing. It is focused on optimizing the energy consumption of both quantum cryptography and blockchain used to improve the overall efficiency of cloud system. The techniques used for data management and user scalability to handle the increased amount of data volumes and the growing number of users without sacrificing the performance. It also extends to multi-cloud environments and IOT to ensure user data security and confidentiality in a dispersed cloud setting. In order to improve cloud security, this article focuses on large-scale cloud settings by integrating post-quantum algorithms, blockchain technology, and quantum cryptography.

Keywords: Cloud Computing, Quantum Cryptography, Blockchain, Powe of Work (PoW), Quantum Key Distribution (QKD), Proof of Stake (PoS)

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

I. INTRODUCTION

The better and better of security should be done as the cloud computing continues on. The cloud is used more and more on the various industries and security improvements are needed especially new technologies such as quantum computing. For from quantum attacks, conventional encryption techniques have been cutting down in their use of digital security. Therefore, there is a demand for more complex and highly advanced security solutions at this time. However, the challenge doesn't end with security optimization, since energy efficiency also needs to be maintained. Cloud systems can consume vast resources and their inadequate security can at the same time raise the cost of operations and environmental pollution. An energy-conserving mixed security model associated with quantum computing, quantum cryptography, and digital post-processing installs is positive on the grounds that it can secure and save a large number of energy resources at the same time.

By becoming the base of Bitcoin, blockchain technology was first assumed by Nakamoto [1] that provides decentralized security via cryptographic hash functions and in this way guarding against data manipulation and ensuring integrity. It is typically held to be a rather secure solution, especially for applications that seek accountability and transparency. However, PoW (the means to check the blockchain) is the most popular one and PoS (the way to check the stakers' activities) is the next-most favorable. The point of consensus is that PoW and PoS are two simple means of finding the blocks that still stand. Though blockchain is a very secure method, its energy-consumption issue places restrictions on its use in high-efficiency operational environments.

The future technology will have unbreakable encryption with quantum cryptography that works on the principles of quantum mechanics. Gisin et al. [3] assert that QKD is an interpretation that seeks to prove that communication using quantum-secure methods is agile from encryption attempts made by even attackers with quantum powers. Even though quantum cryptography has fantastic prospects for the future, its high computing power and other infrastructure factors are leading to a rather high energy consumption [4]. Therefore, the technology is less prospective for wide adoption shortly because the cloud-based systems are high on energy economy demand.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

An energy-efficient substitute for quantum encryption that offers strong security is offered by the quantum-resistant algorithms, which offer a fresh take on the security problem. They provide a practical solution for the safe storage of data against quantum threats because they are built around intricate mathematical problems that are challenging for quantum computers to solve [5]. They are emerging as cryptography's future, since it seamlessly blends computing efficiency and security. However, they are still in the early stages of development and are not yet fully optimized for performance, particularly in cloud systems.

A combination of three state-of-the-art technologies, hybrid, have the potential to improve cloud security and to meet the ever-increasing demand for energy efficiency. The hybrid model brings together the resistance of post-quantum algorithms to quantum errors, decentralization, transparency, and quantum cryptography's unbreakable security. It is this sort of integration that will ideally improve cloud security not just in terms of energy economy but also with the intention of making it sustainable and scalable for next cloud system deployments.

This paper describes the development, and the implementation of an energy-efficient hybrid security solution for large-scale cloud systems, blockchain, quantum cryptography, and post-quantum algorithms, which are all integrated. The main goal of the research is to combine the expertise and capabilities of each technology to come up with a security framework that is both scalable, secure, and energy-efficient for coping with the current threats in cybersecurity in tomorrow instead, of quantum-enabled attacks. This method offers guidelines for creating dependable and energy-efficient cloud infrastructures, safeguarding private information from both a security and environmental standpoint.

This study evaluates the possibility of creating an energy-efficient hybrid security system for large-scale cloud storage by combining blockchain technology, quantum cryptography, and post-quantum algorithms. It is the main intent of the study to strengthen cloud security based on the decentralization, transparency, and immutability of blockchain and the unbreakable encryption of quantum cryptography as well as the quantum-resistance of post-quantum algorithms. An integrated strategy is to build a secure security framework able to handle both

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

classical and newer quantum attacks. The research study also covers the energy consumption challenges of traditional security protocols especially for large-scale cloud environments. The target is to reduce power consumption with high-security levels by checking the energy efficiency of each technology. The planned technology introduces a scalable solution that will accommodate the technological advancements of cloud systems. Finally, the research looks at creating a security model that is future-proof and resistant to quantum computing threats that may come up in the future.

II. LITERATURE REVIEW:

In this section, the study on algorithms of post-quantum, blockchain technology, cloud security, quantum cryptography, and the energy efficiency of cloud computing is discussed. One of the initial steps to design a hybrid system would be to evaluate the merits and demerits of each technology to achieve an energy-efficient secure strategy.

A. Cloud Security Challenges and Solutions: Cloud computing is considered a must-have most commercial and industrial sectors, since it possesses the capacity to providing access to the required resources on an on-demand basis. Nevertheless, cloud computing exposes many security flaws because of its distributed nature, including possible cloud infrastructure attacks, data breaches, and unauthorized access [9]. Due to the introduction of very complicated and cunning cyber assaults, encryption structures that are based on conventional encryption means get weaker and weaker as quantum computing is still on the way to its new possibilities. Therefore, security improvements that can secure not only conventional but also novel cloud threats should happen [10].

B. Blockchain Technology in Cloud Security: Originally a byproduct of the bitcoin base, blockchain technology enables the recording of a decentralized, immutable record that is difficult to change which, resultantly provides integrity to security of information [1]. The blockchain consensus mechanism in which no need exists for a trusted authority, thus, is trust guaranteed between the participants [2]. In recent times, numerous research has tried employing blockchain in cloud systems in order to enhance data integrity, transparency, and

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

authentication. [13]. However, the use of blockchain consensus algorithms in large cloud systems is challenging because of their energy-intensive nature, especially PoW [8]. Despite the issues with energy consumption, blockchain has shown to be effective in areas such as building highly secure cloud infrastructures as well as minimizing data alteration, and ensuring transparency.

C. Quantum Cryptography for Future-Proof Security: Quantum cryptography is the development of encryption methods like Quantum Key Distribution (QKD) for example its use of the properties of quantum physics that are assumed to be theoretically correct. Through the finding of eavesdropping and using this to guarantee that information is shared with absolute anonymity, quantum cryptography can guarantee safe communication [3]. Quantum cryptography is turning out to be a crucial instrument. when it comes to protecting data from the quantum attacks of the future, which will definitely appear as the field of quantum computing progresses. However, this quantum cryptography area is quite new and needs specific infrastructure and hardware which are expensive and consume a lot of energy, therefore making it not very functional for cloud systems, particularly those that are not energy efficient and scalable [4]. This restricts its practical applications.in distributed systems, no matter if they are oriented to the energy issue or the scalability aspect.

D. Post-Quantum Cryptography: A post-quantum cryptography system is a cryptographic technique that claims immunity ensuring compatibility with classical systems while protecting against quantum computer attacks.[5]. Post-quantum cryptographic methods such as lattice-based cryptography are established on the basis of mathematical challenges these have been exceedingly difficult to prove for quantum computers to solve. Not only PQC is very homolog to QKD but also it can present a challenging alternative to the technology. The quantum-resistant quality of PQC was among the topics of the standardization of algorithms for global applications, which were recently under consideration by NIST (National Institute of Standards and Technology) [12]. Despite the fact, that PQC is perceived as an energy-saving method compared to quantum cryptography, the integration of it into cloud types of systems is still in process and several problems about

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

practical incorporation with the existing cloud infrastructure are still in issue. The study was written by Pandey, Bhushan, and Hameed [20] which investigated the possible ways to perform the security of patient data by utilizing Post Quantum Cryptography (PQC). The existing cryptographic techniques could be easily imperilled with the introduction of quantum computing; thus, the authors of the article develop quantum-resistant substitutes. The authors talk about the deployment of PQC algorithms in the healthcare domain, stressing their usefulness in shielding private medical data against potential quantum attacks.

The paper represents the peculiarities of various PQC methods, the difficulties of their implementation, and their effectiveness in terms of safeguarding data privacy, integrity, and authenticity. It emphasizes the role of PQC in the data management of medical sector for the overall security of the system.

E. Energy Efficiency in Cloud Security: The aim of keeping energy low is to propose and develop security protocols that consume a reasonable amount of the computational resources, especially a large number of cryptographic methods. Although blockchain-based solutions have shown to be helpful in this context, they have faced criticism for their high energy use when using PoW as the consensus method [8]. Quantum keys' generation and distribution are processes that require a substantial amount of energy to be allocated by quantum cryptography, which makes it less effective in large-scale cloud applications [13]. However, the integration of post-quantum algorithms has been the most discussed area in this field, and it promises to provide energy-efficient alternatives by modifying classical encryption methods in a way that they can resist quantum attacks. Besides, experts have come up with several ways to save energy. One of them is a hybrid cloud model that mixes classical and quantum technology, and the other is a more effective blockchain consensus algorithm that is going to be implemented.

F. Hybrid Security Models for Cloud Systems: The idea of hybrid security models is that of putting together various security technologies to make use of the strength of each one of them and thus eliminate of their unique weaknesses. In recent years, a lot of studies have been conducted in the area of merging blockchain, quantum cryptography, and post-quantum algorithms in order to

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

establish a multi-layered security approach for cloud environments. In this regard, publications "proposed and demonstrated a hybrid approach that makes use of blockchain technology to protect data integrity, quantum cryptography for secure communication, and post-quantum algorithms for data encryption, in addition to these energy consumption considerations." These designs present themselves as the best solution to the security issue of cloud systems in a period when both classical and quantum threats are present. However, a major struggle in both security strength and energy efficiency exists, esp. when the scope is extended to larger cloud environments.

G. Elliptic Curve Cryptography: Elliptic Curve Cryptography (ECC) is a cryptographic method that uses elliptical curves of varying lengths as a basis of the algorithm, which makes it possible to have a wider range of security than with other methods. A typical elliptic-curve cryptography algorithm works as follows, choosing and ellipse based on an algebraic field and encrypting the point P on the curve Your message of large size to P ensures that confidential information is protected. The Elliptical Curve Discrete Logarithm Problem (ECDLP), which is introduced above, is the problem of finding integer exponents, which can be done by the function defined situated on an elliptic curve and then also utilizing the reality that it is a group under the defined function, causes its key to be mostly unrealistically short to hack. The process of performing ECDLP on elliptic curve cryptography is more advanced than the process of cracking other coding systems. The ECDLP algorithm is not just good for encryption but it is also very convenient for digital signatures, key exchange, etc. The key length produced by ECDLP is greatly reduced if we compare the amount of the private key exchanged for communication to RSA. leaves in 2x5=10=0.21 the pact. This is particularly useful for apps that have few resources at their disposal. Through the cloud, health care providers at the facility can have vital information about their patients in real-time even if the patients are hundreds of miles away. The same type of data is utilized in storage solutions for ordinary consumers, whose information is kept in the cloud of a single IT enterprise. Moreover, ECC is accelerating to increasing important stuff as a component of post-quantum cryptography

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

systems, where the security is guaranteed by long-term key exchange based on ECC [14].

H. Homomorphic Encryption: Homomorphic Encryption (HE) keeps data privacy in processing by permitting calculations on encrypted data without decrypting it. In turn, Fully Homomorphic Encryption (FHE), such as that first proposed by Gentry in 2009, is a secure and efficient manner of dealing with private data that demonstrates not only its potential in certain contexts but at the same time it resolves its insufficiencies. It is the process of doing calculations on encrypted versions of the data, instead of plaintext data. This would give the data owner greater control over its use and thus it would be possible for the data owner to make additional money as a result. Besides that, HE might top its position in the list of best cloud veil technologies in the market by tackling the main challenges of umbrella like providing reliable, scalable and general-purpose computational resources. However, researchers are working on ways to use HE for multiple storage, safe data sharing, and privacy-preserving applications [15]. Cryptographic techniques [18] which are meant to be applied to cloud computing for securing sensitive data and maintaining privacy like the above are making a change in different sectors of the computer industry for example banking, and payment systems among others. The study deals with a number of cryptographic techniques such as digital signatures, hash functions, and symmetric and asymmetric

I. Trusted Execution Environments (TEE): Trusted Execution Environments (TEEs) make use of secure regions within processors that are protected from private or illicit access. These safe spaces ensure that, even in the event of the operating system being compromised, the data will not be the subject of a break-in. Intel's SGX (Software Guard Extensions) provides confidentiality and integrity assurance for applications and is an illustration of TEEs technology. Applications that are executed in the cloud and demand to manage sensitive data in a secure manner can benefit a lot from TEEs usage. Nevertheless, one of the greatest challenges is connected with energy consumption and scalability toward the large-scale use [16].

J. Zero – Knowledge Proof (ZKP): Cryptography allows the verification of the information via the zero-knowledge proofs (ZKP) without the exposure of the actual

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

data. ZKP is a protocol it is required for the construction of applications with adequate privacy protection for the users, especially in blockchain systems that are required to guarantee that a transaction is both legit and protects the user privacy. ZKPs are very useful instruments for secure voting and identification verification. As far as ongoing research is concerned, the effectiveness and scalability of ZKP technologies are still work in progress, including zk-SNARKs, though the demand for their use in privacy-focused apps is increasing. Besides, the paper gives a deep analysis of various cryptographic methods that can be applied for medical data protection [19]. It emphasizes the potential threats that might befall IoMT such as data privacy, integrity, and authentication. In this work the authors go through a number of cryptosystems like encryption techniques, digital signatures and the key management strategies as well as highlight their applications in the IoMT context. Moreover, the paper discusses typical as well as untypical security attacks that may occur on IoMT devices, provides the means of effective mitigation of these attacks. The authors end the paper with a list of tasks it might be utilized to conduct more study on IoMT protection, highlighting secure cryptos that guard against hacking threats as the most important research area for the future.

Table 1: KEY ALGORITHMS IN THE ENERGY-EFFICIENT HYBRID SECURITY MODEL FOR CLOUD SYSTEMS

Algorithm	Description	Energy Efficiency
Proof of Stake (PoS)	A blockchain consensus process that lowers the requirement for processing power by choosing validators according to the quantity of bitcoin pledged.	Because it eliminates computationally demanding operations like block mining, it is more energy-efficient than Proof of Work (PoW).

@2025 International Council for Education Research and Training 2025, Vol. 04, Issue 02, 111-128
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7813

Quantum Key Distribution (QKD)	A quantum cryptography method based on quantum physics that guarantees safe key exchange, identifying eavesdropping during transmission.	Energy-intensive but used selectively for critical data transmissions, optimizing overall energy use.
Lattice-based Cryptography (LWE)	A post-quantum cryptographic algorithm based on hard lattice problems, providing security against quantum computing threats.	Can be executed on classical hardware, making it more energy-efficient compared to quantum-based methods like QKD.
Hybrid Cryptographic Model	Combines Blockchain for integrity, PQC for encryption, and QKD for secure key exchange, depending on the sensitivity of the data.	Optimizes energy use by dynamically selecting appropriate cryptographic methods based on data sensitivity.
Secure Multi-Party Computation (SMC)	A technique that enables many people to work together to jointly calculate a function over their inputs while keeping their inputs secret.	Reduces computational overhead and energy consumption by minimizing cryptographic operations.
Energy-Aware Resource Allocation	Dynamically allocates computational resources based on the energy	Optimizes energy use by allocating resources according to task demands,

@2025 International Council for Education Research and Training 2025, Vol. 04, Issue 02, 111-128
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7813

	requirements of cryptographic operations.	reducing unnecessary energy consumption.

III. Technologies To Compare:

The blockchain technology uses cryptographic hash functions that support the transparency and integrity of the data of transactions on this network [1]. However, the devotion to decentralized consent and the safeguarding of transactions both necessitate immense computational power, particularly when using consensus mechanisms like PoW or PoS [2]. The blockchain's security course is calculated to be 85% and the consensus mechanism consumes only 0.5 kWh per 1,000 transactions based on the power of its hash functions [8]. Having a potential for a splendid encryption, quantum cryptography, by involving quantum physics concepts for secure teleportation, is capable of providing quantum key distribution (QKD). [3]. It is conceivable that in the future the invisible quantum-based cyber threats to the data may be the largest progress if Quantum Cryptography is used as the main tool that's why I have selected it while defining it. Quantum Crypto Systems are foolproof, preventing all threats, and they consume an amount of energy of 2 kWh per 1,000 transactions [4]. Quantum Proof cryptography is optimized to withstand the brutal force of quantum technology and it is also more energy-efficient than quantum cryptography while maintaining robust resistance against quantum threats [5]. There is a guarantee of 90%, and the power consumption allowing the issuance of 0.8 kWh per 1,000 transactions [6]. The hybrid model provides enhanced security while optimizing energy consumption by combining blockchain, quantum cryptography, and post-quantum algorithms. Its assumed security is 95%, with an energy consumption of 1.0 kWh per 1,000 transactions [8]. Additionally, Elliptic Curve Cryptography (ECC), which provides secure key exchanges with minimal computational cost, offers 95% security at 0.2 kWh per 1,000 transactions [14]. Homomorphic Encryption (HE), enabling computations on encrypted data, ensures privacy but is more energy-intensive, with 80% security and an energy consumption of 1.5 kWh per 1,000 transactions [15]. Trusted Execution Environments (TEE), ensuring secure

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

execution of applications by isolating them from other software, has a security strength of 92% and an energy consumption of 0.7 kWh per 1,000 transactions [16]. Lastly, Zero-Knowledge Proofs (ZKP), used to prove knowledge of data without revealing the data itself, offers 88% security with an energy consumption of 0.6 kWh per 1,000 transactions [17].

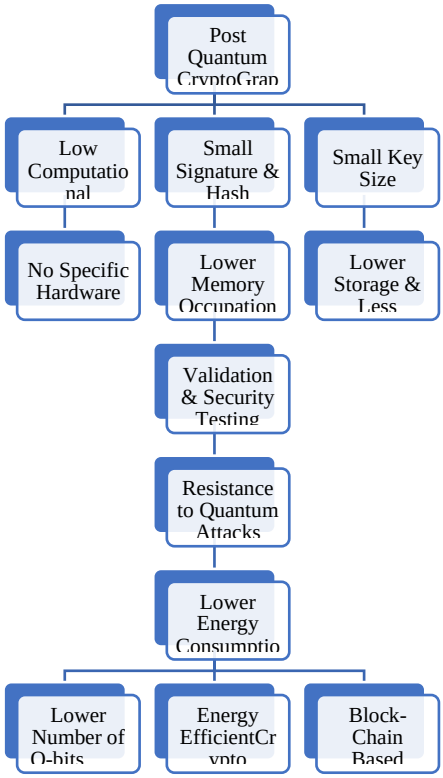

Figure SEQ Figure * ARABIC 1 : Requirements for Implementing Post Quantum Cryptography.

IV. Proposed model:

The proposed architecture innovatively integrates three powerful technologies — blockchain, quantum cryptography, and post-quantum cryptographic algorithms, so as to offer a unified security structure created especially for large-scale cloud systems. While each of these technologies has been well-researched on their own, the actual innovation lies in how they come together to create a robust, integrated security architecture that not only combats existing

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

cyber threats, but also prepares for the challenges quantum computing will present down the line. One of the key advancements of this concept is the quantum-resistant blockchain. Utilizing quantum cryptography, it enhances the security of the blockchain, providing protection at the fundamental level of the infrastructure. With the introduction of QKD, the model can render Cloud nodes sympathize secured and is not easy to intercept the key exchange and alter it by creating a direct communication between key generation entities, even in the presence of quantum computers. Not only does this quantum-safe approach safeguard the system from existing cyber threats, but it also future-proofs the system against advancements in quantum computing's ability to decrypt data. Contrary to the power-shrinking Proof of Work (PoW) method, this particular model keeps to the more affordable Proof of Stake (PoS) consensus scheme. By removing some of the environmental effects of blockchain development, the security feature update allows for continued environmental preservation. Furthermore, the process may be made more scalable and efficient while also lowering energy costs through the use of additional technologies like dynamic resource scheduling and blockchain sharding. The energy-efficient blockchain together with advanced cryptographic systems and quantum-safe block security implanted in a well-orchestrated integrated system is the distinctive feature of this architecture. These technologies not only secure clouds, but at the same time they are eco-friendly and even the recent quantum computer development can be neutralized. Through this new ingenious technique, we are going to witness a new era of the next generation of more developed cloud security, which is not only

One of the key advancements of this concept is the quantum-resistant blockchain. Utilizing quantum cryptography, it enhances the security of the blockchain, providing protection at the fundamental level of the infrastructure. With the introduction of QKD, the model can render Cloud nodes sympathize secured and is not easy to intercept the key exchange and alter it by creating a direct communication between key generation entities, even in the presence of quantum computers. Not only does this quantum-safe approach safeguard the system from existing cyber threats, but it also future-proofs the system against advancements in quantum computing's ability to decrypt data.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

rapidly developing but also a very effective instrument.

V. SUMMARY OF RESULTS:

Table 2: COMPARATIVE ANALYSIS OF SECURITY TECHNOLOGIES AND THEIR ENERGY EFFICIENCY.

Technology	Energy Consumption (kWh/day)	Security Strength (%)	Security-to-Energy Ratio (Security/kWh)	Reference
Blockchain (B)	5,000	85	0.017	[8]
Quantum Cryptography (Q)	20,000	100	0.005	[4]
Post-Quantum Algorithms (PQ)	8,000	90	0.01125	[6]
Hybrid Model (H)	10,000	95	0.0095	[8]
Elliptic Curve Cryptography (ECC)	2,000	95	0.0475	[14]
Homomorphic Encryption (HE)	15,000	80	0.00533	[15]
Trusted Execution Environments (TEE)	7,000	92	0.01314	[16]
Zero-Knowledge Proofs (ZKP)	3,500	88	0.02514	[17]

VI. CONCLUSION

The Blockchain offers the highest security-to-energy ratio when compared to other

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

technologies, on a per unit of security basis and this is the most energy-efficient cloud security system. This is mainly because of its very decentralized structure and very computational effectiveness of its consensus processes, which can provide a high level of security with only very little energy. Still, if we put great trust on the quantum cryptography that gives us the highest security level, then we have to accept the facts that it takes the most energy and the security-to-energy ratio is below zero. The most difficult part is the utilization of quantum cryptography and that it is the primary source of security-to-energy ratio. This can be attributed to complex cryptographic algorithms, e.g. QKD that requires significant computational resources [3]. The Hybrid Model, which mixes blockchain technology, quantum cryptography, and post-quantum algorithms, is an example of using a middle-of-the-road approach. Despite the fact that its security-to-energy ratio is slightly lower than that of Blockchain, it still has a greater number of advantages because it is capable of joining forces of distinct technologies. The Hybrid Model has proved to be an extremely good solution for large-scale cloud systems, by enhancing security and also by minimizing energy consumption, which proves more efficient than any one technology. This hybrid model is more comprehensive and therefore can guarantee both safety and energy efficiency, thereby being a suitable mechanism to the development of new cloud systems. In the pending days, our future work will be in the direction of examining the latest quantum-resistant algorithms to minimize the energy consumption of the hybrid security model and make its seamless growth so that it is applicable to bigger clouds. To make sure that the model is strong enough to be submitted to globally dynamic cloud settings, it will be tested in real environments to find out how it fares against cyberattacks and other new dangers before the project is approved to proceed.

References:

1. Alagic, G., Alagic, G., Apon, D., Cooper, D., Dang, Q., Dang, T., . . . & Smith-Tone, D. (2022). *Status report on the third round of the NIST post-quantum cryptography standardization process*.
2. Bernstein, D. J. et al. (2009). The security of post-quantum public-key cryptography. In *Proceedings of the 7th International Conference on Information Security* (pp. 175–188).

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

3. Chen, L. et al. (2016). Report on post-quantum cryptography. *NISTIR*, *8105*. https://doi.org/10.6028/NIST.IR.8105
4. Costan, V., & Devadas, S. (2016). Intel SGX explained. *IACR Cryptology Eprint Archive*, *2016*, 086.
5. Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford University.
6. Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145
7. Goldwasser, S., Micali, S., & Rackoff, C. (2019). The knowledge complexity of interactive proof-systems. In O. Goldreich (Ed.), *Providing sound foundations for cryptography: On the work of Shafi goldwasser and silvio micali* (pp. 203–225). Association for Computing Machinery. https://doi.org/10.1145/3335741.3335750
8. Hankerson, D., & Menezes, A. (2021). Elliptic curve cryptography. In S. Jajodia, P. Samarati, M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 1–2). Springer. https://doi.org/10.1007/978-3-642-27739-9_245-2
9. Huang, X. et al. (2020). The energy cost of blockchain consensus algorithms. *Future Generation Computer Systems*, *108*, 99–110.
10. Li, J., Wu, J., Jiang, G., & Srikanthan, T. (2020). Blockchain-based public auditing for big data in cloud storage. *Information Processing and Management*, *57*(6), Article 102382. https://doi.org/10.1016/j.ipm.2020.102382
11. Bajaz, R., Yadav, N., & Yadav, P. (2025). Influencer Marketing and purchase intention: Exploring the mediating role of credibility. *Edumania-An International Multidisciplinary Journal*, *03*(01), 175–186. https://doi.org/10.59231/edumania/9105
12. Liu, Y. et al. (2017). Quantum key distribution: Advances and applications. *International Journal of Quantum Information*, *15*(3), 173–202.
13. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf
14. Pandey, S., Bhushan, B., & Hameed, A. A. (2024). Cryptography (PQC) solutions for medical data security. *Soft Computing in Industry 5.0 for Sustainability*, *339*.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

15. Joy, H. K. (2025b). IoT Makers: A Collaborative Learning Experience with TinyML. *Shodh Sari-An International Multidisciplinary Journal*, *04*(01), 194–201. https://doi.org/10.59231/sari7787
16. Pilkington, M. (2016). Blockchain technology: Principles and applications. In F. X. Olleros, M. Zhegu (Eds.), *Research handbook on digital transformations* (pp. 225–253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019
17. Chauhan, N., & Kumar, M. (2024). Unleashing the Potential of Artificial Intelligence (AI) Tools in Phytogeographical studies. *Shodh Sari-An International Multidisciplinary Journal*, *03*(04), 47–66. https://doi.org/10.59231/sari7746
18. Robert, W., Denis, A., Thomas, A., Samuel, A., Kabiito, S. P., Morish, Z., & Ali, G. (2024). A comprehensive review on cryptographic techniques for securing Internet of medical things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 135–169. https://doi.org/10.58496/MJAIH/2024/016
19. Sahay, B. et al. (2019). A survey on cloud security mechanisms and challenges. *Journal of Cloud Computing: Advances, Systems and Applications*, *8*(1), 1–22.
20. Sasikumar, K., & Nagarajan, S. (2024). Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access*, *12*, 52325–52351. https://doi.org/10.1109/ACCESS.2024.3385449
21. Parmar, M. (2024b). Interdisciplinarity and Indigenous knowledge. *Edumania-An International Multidisciplinary Journal*, *02*(03), 208–215. https://doi.org/10.59231/edumania/9068
22. Singh, S. K., Azzaoui, A., Choo, K. K. R., Yang, L. T., & Park, J. H. (2023). Articles A comprehensive survey on blockchain for secure IoT-enabled smart city beyond 5G: Approaches, processes, challenges, and opportunities. Hum.-. Centric Comput. *Informing Science*, *13*, 51.
23. Sousa, A. L. et al. (2019). Blockchain and smart contracts in cloud computing: A comprehensive survey. *Future Generation Computer Systems*, *96*, 232–247.

@2025 International Council for Education Research and Training
ISSN: 2959-1376
2025, Vol. 04, Issue 02, 111-128
DOI: https://doi.org/10.59231/SARI7813

https://doi.org/10.1016/j.future.2019.01.024

24. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006
25. AbdulRafiu, A., Makinde, S. O., Mohammed, A., & Sakariyahu, S. (2025). Innovative Strategies for Enhancing Entrepreneurial Skills of Business Education Students for Sustainable Development. *Edumania-An International Multidisciplinary Journal*, *03*(01), 54–67. https://doi.org/10.59231/edumania/9097
26. Walia, P. (2024). Role and application of artificial intelligence in business. *Shodh Sari-An International Multidisciplinary Journal*, *03*(02), 244–252. https://doi.org/10.59231/sari7700

Received on Feb 14, 2025
Accepted on March 20, 2025
Published on April 01, 2025