Gəlin yaşıl innovasiyaların verdiyi imkanlardan istifadə edək və hamı üçün daha parlaq, daha davamlı gələcək formalaşdıraq.

Nəticə

Yaşıl texnologiyaların tədqiqi innovasiya və potensialla zəngin mənzərəni ortaya qoyur. Bu texnologiyalar sadəcə tendensiyalar deyil, onlar davamlı gələcəyin formalaşdırılmasının ayrılmaz hissəsidir. Bərpa olunan enerjidən yaşıl arxitekturaya qədər hər bir inkişaf ətraf mühitin qorunmasına və davamlı həyata əhəmiyyətli töhfə verir. Çətinliklər, texnoloji irəliləyişlər və davamlılığa doğru ictimai düşüncə dəyişikliyi ilə tədricən həll olunur . Biz irəlilədikcə yaşıl texnologiyaların həyatımızda rolu daha qabarıq şəkildə özünü büruzə verəcək və ekoloji şüurun və məsuliyyətin yeni dövrünü müjdələyəcək. Yaşıl texnologiyaların yüksəlişi həm planetimiz, həm də həyat keyfiyyətimiz üçün perspektivli gələcəyi nümayiş etdirir. Günəş enerjisi innovasiyaları, qabaqcıl enerji saxlama həlləri, karbon tutma texnologiyaları, tullantıdan enerjiyə çevrilən nailiyyətlər və yeni nəqliyyat konsepsiyaları vasitəsilə dünya davamlılıq dövrünə yaxınlaşır. Fəaliyyətlərimizdə və siyasətlərimizdə yaşıl texnologiyaya üstünlük verməyə davam etdikcə, daha parlaq, daha dayanıqlı gələcək üçün potensial əlimizdən düşür.

Ədəbiyyat siyahısı.

[1] AAI (2022). Africa adaptation initiative. Africa Adaptation Initiative (AAI). Available at: https:// africaadaptationinitiative.org [accessed August 2022].

[2] Abdel-Shafy, H. and M. Mansour (2013). Overview on water reuse in Egypt: Present and future. J. Sustainable Sanitation Practice, 14,.

[3] Adaptation Fund (2022). Innovation funding. Adaptation Fund. Available at: www.adaptationfund.org/apply-funding/innovation-grants [accessed September 2022].

[4] Sanjukta Banerjee, Yaşıl texnologiyanın üstünlükləri , (2014).

[5] Will Kenton, Green Tech , I NVESTOPEDIA . COM (2020), Green Tech Davud Popp, The Rol of Yaşıl Texnologiya Transfer in İqlim Siyasət. (2010),

[6] Cleantech Group (2021). Genetic engineering for crops and food: Climate adaptation, resilience, and food security through innovation. Available at: www.cleantech.com/genetic-engineering-forcrops-and-food-climate-adaptation-resilience-and-food-security-through-innovation [accessed October 2022].

[7] Climate-ADAPT (2015a). Adaptation or improvement of dikes and dams. The European Climate Adaptation Platform Climate-ADAPT. Available at: https://climate-adapt.eea.europa.eu/metadata/ adaptation-options/adaptation-or-improvement-of-dikes-and-dams [accessed July 2022].

[8] FAO (2015). Climate change and food security: Risks and responses. Rome: Food and Agriculture Organization of the United Nations (FAO). Available at: www.fao.org/3/i5188e/I5188E.pdf.

[9] FAO (2017). Chinese scientists develop rice that grows in seawater, potentially creating food for 200 million people. Food and Agriculture Organization of the United Nations (FAO). Available at: www.fao.org/in-action/agronoticias/detail/en/c/1060351 [accessed October 2022].

POST-QUANTUM CRYPTOGRAPHİC METHODS FOR SECURİNG IOT DEVİCE

Mammadaliyeva G.N.

Azerbaijan State Oil and Industry University

The Internet of Things (IoT) is growing at a rapid pace, and quantum computing will eventually develop, which will help to secure IoT devices. Post-quantum cryptography (PQC) techniques are necessary because quantum algorithms have the potential to undermine traditional encryption techniques. This article addresses the risks to Internet security that quantum computing presents and looks at PQC methods to reduce those risks [2]. The vulnerability of contemporary cryptographic algorithms to quantum assaults is first discussed in the article, followed by the necessity of finding substitute techniques. After that, he examines the fundamentals of multivariate polynomial cryptography, code, lattice-based cryptography, and hash functions. The foundation of all approaches is their ability to withstand quantum assaults and the fact that they can be implemented in Internet devices with constrained capabilities.Performance concerns, interoperability with current protocols, and the deployment of post-quantum cryptography solutions on the Internet are all covered in the paper. It also talks about the continuous attempts to standardize PQC standards, which guarantee uniformity and simplicity of quality across different Internet of Things (IoT) platforms **Keywords:** post-quantum cryptography, quantum computing, IoT security, lattice-based cryptography, code-based cryptography, hash-based cryptographyTechnology has altered our interactions with it by allowing data interchange and physical connectivity between Internet of Things (IoT) devices. From smart household appliances to industrial control systems, the Internet of Things is influencing many facets of contemporary life. Still, a lot of major issues have arisen as a result of the Internet's explosive growth, particularly in the areas of privacy and security [4].

Conventional internet security techniques, including RSA and ECC, rely on classical cryptography to protect data and communications. Although these methods have a track record of successfully protecting networks and devices connected to the Internet, the quantum computing demonstration may render them outdated. Modern cryptographic computer methods are susceptible to quantum attacks, which exposes Internet systems to danger [5].

Strong substitutes that can withstand portable quantum assaults are post-quantum cryptography techniques. In spite of the difficulties posed by quantum computing, methods like hash, code, and lattice cryptography offer a reliable means of protecting networks and devices connected to the Internet [3].

This article's goal is to investigate post-quantum cryptography techniques for Internet security. We'll examine a few of post-quantum cryptography algorithms, assess their suitability and efficacy for the Internet of Things, and talk about the potential and problems associated with spearheading them. Our study aims to uncover methods that are used in the real world. Post-quantum cryptography can contribute to the long-term security and integrity of data, as well as the robustness of Internet networks [8].

AIM: The goal of this article is to provide current research and industry concepts while arming readers with the knowledge and resources they need to navigate the rapidly changing field of quantum-resistant security solutions. This demonstrates that in the quantum age, taking preventative actions is crucial to safeguarding Internet-connected devices against new threats.

METHODS

Post-quantum cryptography approaches safeguard communications and data when quantum military threats compromise cryptography systems. As quantum computing advances, current encoding standards like RSA and ECC may be susceptible to quantum assaults. Even with processing power, post-quantum cryptography provides solutions to mathematical puzzles [1].

Among the post-quantum cryptography techniques are the following:

Lattice-based cryptography: This technique makes use of many lattice issues, including the learning with error (LWE) problem and the smaller vector problem. Since it is thought that quantum computers would not be able to tackle these issues, lattice-based cryptography is a potential solution for safeguarding Internet-connected devices. The cryptosystem's flexibility stems from its utilisation of digital signatures, key exchange, and continuous encryption lattices. On the other hand, their application could have more significant effects on how well Internet of Things (IoT) devices operate and use resources [1].

Code-based cryptography. Code-based encryption complicates the process of decoding a random linear code. Goppa binary codes may be encrypted using the most well-known code-based cryptosystem, McEliece. In the realm of security and defense against quantum assaults, this technique is well-known. Even though code-based cryptosystems have many benefits, large public key sizes might not be enough in an Internet setting with limited resources [1].

Hash-Based Cryptography. Secure primitives like digital links are created by hash-based cryptography, which makes use of hash encryption techniques. One popular hash-based connection mechanism is the Lamport-Diffie one-time signature. It has been demonstrated that these tactics work well and are immune to quantum assaults. On the other hand, if one-time keys are used frequently, they could degrade management keys and storage capacity [1].

Multivariate Polynomial Cryptography. The difficulty of system solutions to high-dimensional polynomial models over finite fields serves as the foundation for this tactic. Multivariate polynomial cryptography's quick calculation and small key sizes make it appropriate for Internet devices with constrained resources. However, furnace patterns are not always changeable, therefore technique selection is crucial [1].

Integration with IoT Devices

Post-quantum cryptography measures must be included into Internet devices in order to safeguard these systems against new dangers arising from quantum computing. However, this integration presents several obstacles because of the Internet of Things and other devices [7].

The processing speed, memory, and power consumption of many devices on the Internet are constrained. Larger key sizes and more intricate computations are common in post-quantum cryptography techniques, which can be difficult for hardware with limited power. The improvement of algorithms for gauging productivity and resource use is required to address this issue [6].

Interacts with third-party protocols and communication standards that are now in use in Internet ecosystems, such as MQTT, CoAP, and Zigbee. When creating, expanding, or altering documents that can support post-quantum cryptography approaches, certain protocols must be taken into consideration [7].

Make sure you keep an eye on network connectivity, latency, and bandwidth. Performance and security must be combined in cryptographic techniques to guarantee dependable and effective international transactions. Key management strategies are necessary to generate, distribute, store, and rotate the bigger keys that are frequently connected to post-quantum cryptography in order to protect the privacy and integrity of communications [4].

To assist clients, a thorough security architecture that incorporates access control, data encryption, and device authentication must be developed. As a result, the security foundation for Internet systems becomes more solid and cohesive.

To guarantee network device security, optional firmware upgrades and lifecycle management are also required. Secure over-the-air updates are required to repair security gaps and improve system stability when using post-quantum cryptography techniques [10].

Thorough testing and setup are necessary to guarantee correct interoperability with current networks and applications. Compatibility, security, and performance ratings are included in this section. A straightforward and open management method is essential to avert needless issues and preserve a positive customer experience [2].

RESULTS

Strengthening IoT Security: Exploring Post-Quantum Cryptography

This article looks at the most recent advancements in Internet of Things security as well as the upcoming quantum computing age. It also investigates the effectiveness of post-quantum cryptography (PQC) methods for Internet of Things device security. He draws attention to the fact that conventional cryptography methods are susceptible to quantum assaults and emphasizes the significance of developing quantum-proof solutions [9].

The article begins with a summary of the revolutionary possibilities of quantum computing before delving into the fundamentals of post-quantum cryptography, covering lattice, code, hash, and multidimensional polynomial cryptography. It assesses the degree to which these techniques effectively shield Internet-connected devices from quantum radiation as well as their resistance to it.

Conclusion

In conclusion, it should be highlighted that post-quantum cryptographic techniques must be included into Internet of Things devices in order to safeguard Internet of Things systems from risks brought on by quantum computing. By using methods like hash-, lattice-, and code-based encryption, the Internet of Things may be made more resilient and secure. Even while challenges like resource Sconstraints, key management, and interoperability with legacy protocols must be addressed, future-proof security systems provide more benefits than drawbacks. The Internet ecosystem may be strengthened and made more secure by cooperation and innovation, allowing for dependable operation and quantum data security [2].

References:

[1] Albrecht, M., & Fitzpatrick, R. (2019). "Post-Quantum Cryptography: An Overview for Practitioners." IEEE Security & Privacy, 17(3), 12-20.

[2] Al-Khalil, A., & Abdelhakim, S. (2022). "Security Challenges and Future Directions in Internet of Things." IEEE Internet of Things Journal, 9(3), 1235-1247.

[3] Al-Khaleel, S., & Qawasmeh, R. A. (2019). "Internet of Things Security: Fundamentals, Techniques, and Applications." Wiley.

[4] Bahrami, M., & Singhal, M. (2019). "Securing the Internet of Things: A Security Taxonomy for the IoT Environment." Elsevier.

[5] Bernstein, D. J., Lange, T., & Schwabe, P. (Eds.). (2009). "Post-Quantum Cryptography." Springer Science & Business Media.

[6] Chen, Y., & Hu, Y. (2020). "Securing IoT Devices: Insights and Best Practices." Journal of Computer Security, 28(3), 235-249.

[7] Kelsey, J. (2016). "Post-Quantum Cryptography: Third International Workshop, PQCrypto 2016, Fukuoka, Japan, February 29–March 1, 2016, Proceedings." Springer.

[8] Lyubashevsky, V., Peikert, C., & Regev, O. (2010). "A Toolkit for Ring-LWE Cryptography." Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 35-54). Springer, Berlin, Heidelberg.

[9] Mosca, M. (2018). "Post-Quantum Cryptography: Ready for Prime Time?" ACM Queue, 16(1), 44-63.

[10] Proos, J., & Zalka, C. (2003). "Shor's Discrete Logarithm and Factoring Algorithms." Quantum Information & Computation, 3(4), 317-344.

ÇATBOTLAR VƏ VIRTUAL KÖMƏKÇİLƏR

Niftalıyev Eşqin Xaləddin
Azərbaycan Dövlət Neft və Sənaye Universiteti

Abstract

Hal-hazırkı dövrdə texnologiyanın inkişaf etdiyi zamanda çatbotlar və virtual köməkçilər hər bir sahədə istifadə olunaraq texnologiya ilə əlaqəmizdə qarşılıqlı inqilab etmişdir. Süni intellekt və təbii dil emalı ilə təchiz edilmiş bu ağıllı sistemlər insan dilini başa düşə bilir həmçinin ona cavab verə bilir. Siri və Alexa kimi məşhur virtual köməkçilərdən tutmuş müştəri xidməti və səhiyyə sahəsində geniş istifadə olunan ixtisaslaşmış çatbotlara qədər süni intellektlə idarə olunan həllər müxtəlif sahələri dəyişdirir.