DSIM

Enhancing Identity Authentication in Quantum Networks

VAJRATIYA VAJROBOL[1], Ahmad Nur Badri [2], Ika Apriyanti[3]
[1]International center for AI and Cyber Security Research and Innovation, Asia University.
[2]Department of computer science, Esa Unggul University, Indonesia; badrijkt@gmail.com
[3]Department of computer science, Esa Unggul University, Indonesia; ikaapriyantiinka@gmail.com

Corresponding author: First A. Author (e-mail: vvajratiya@gmail.,com).

ABSTRACT Identity authentication is important for secure communications, especially in the era of quantum networks, where traditional methods face new vulnerabilities. This article investigates the evolving landscape of identity verification within quantum networks. Leveraging quantum mechanics, quantum key distribution (QKD) protocols enhance security by generating tamper-proof cryptographic keys. However, QKD alone cannot address all aspects of identity authentication. To address this, the article introduces a Secure Quantum Identity Authentication Protocol that combines QKD with classical encryption, creating a multi-layered, quantum-resistant authentication system to safeguard identity verification in quantum networks.

KEYWORDS Quantum Networks, Identity Authentication,Quantum Key Distribution (QKD), Secure Identity Verification

I. INTRODUCTION

The emergence of quantum networks has become a transformational breakthrough in the fast developing world of modern technology. These networks utilize the distinctive characteristics of quantum physics to facilitate highly secure communication and transmission of data [1]. Quantum networks have the capacity to profoundly transform sectors such as banking, healthcare, and national security, making them highly likely to be widely embraced. Nevertheless, the introduction of this technology also presents new difficulties, with the most significant one being the requirement for strong identity verification inside this quantum domain.

Identity identification is a crucial component of secure communication, guaranteeing that only authorized users are granted access to confidential data and services. Within the realm of quantum networks, conventional authentication techniques frequently prove inadequate in delivering the necessary degree of security to safeguard against advanced cyber attacks [2]. The advent of quantum computing, which has the ability to surpass classical encryption methods, intensifies the need for the creation of novel and quantum-resistant identity authentication protocols.

This article examines the important connection between quantum networks and identity authentication, investigating the difficulties, resolutions, and consequences of safeguarding identities in the quantum age. This provides a concise outline of the article's organization, giving readers a clear guide to traverse this crucial discourse in the ever-changing field of quantum technology and security.

II. Principles of Quantum Networking

Quantum networks are the foundation of a state-of-the-art technological landscape where quantum mechanics plays a central role. These networks are specifically engineered to utilize the fascinating characteristics of quantum particles, such as superposition and entanglement, in order to facilitate safe and high-speed communication over extensive distances [3,4]. Quantum networks, in contrast to classical networks, utilize qubits instead of bits. Qubits have the ability to concurrently represent several states, rendering them more potent for data transmission and processing.

The fundamental concepts of quantum communication in these networks involve the safe transfer of information using quantum key distribution (QKD) protocols. These protocols rely on the no-cloning theorem and the uncertainty principle to ensure the confidentiality and reliability of sent data [5]. The potential of quantum networks extends beyond their capacity to carry information securely, as they also have the power to transform several domains, including cryptography and secure data transfer in sectors such as healthcare and finance.

The significance of security in quantum networks cannot be emphasized enough, given their revolutionary potential. The advancement and use of quantum technologies create fresh opportunities for cyber threats and assaults. With the ongoing progress of quantum computing, traditional encryption techniques may become susceptible, underscoring the importance of implementing strong security measures in quantum networks. This essay will examine the importance of security in quantum networks and explore novel ways to tackle these difficulties.

III. Quantum networks employ identity authentication protocols.

Identity verification is a fundamental aspect of ensuring secure communication, and with the emergence of quantum networks as a cutting-edge technology, authentication methods are also undergoing advancements [6]. Conventional authentication approaches, mostly relying on classical cryptography, are encountering growing difficulties in the era of quantum computing [7]. The potential of quantum computing to undermine traditional encryption techniques presents a substantial danger, emphasizing the necessity for a fundamental change in identity verification methods inside quantum networks.

Ensuring identity identification in quantum networks is a difficult task because of the distinct characteristics of quantum physics [8]. Traditional approaches frequently depend on cryptographic methods that presuppose the confidentiality of keys. However, quantum phenomena like as entanglement and the no-cloning theorem add new aspects of security and privacy. The task at hand is creating authentication techniques that utilize the unique characteristics of quantum systems to create confidence and confirm identities in a setting that fundamentally differs from traditional communication networks.

Quantum physics is crucial in reinventing authentication in quantum networks. Quantum entanglement and superposition principles allow for the generation of cryptographic keys that possess inherent security against interception and manipulation. Quantum key distribution (QKD) protocols, such as BBM92 and E91 protocols, exploit quantum phenomena to create secure communication channels [9,10] and verify the identities of the persons involved. With the ongoing progress of quantum technologies, it is imperative to utilize quantum mechanics in authentication techniques. This not only becomes necessary but also serves as a potent means to guarantee the security and privacy of quantum network communications.

IV. Quantum Key Distribution (QKD)

Quantum Key Distribution (QKD) is a leading secure communication mechanism in quantum networks. The foundations of this technology are based on the laws of quantum physics, enabling the secure exchange of cryptographic keys at an unparalleled degree of security. Quantum Key Distribution (QKD) is based on the inherent characteristics of quantum particles, particularly photons, to generate keys that are impervious to decryption [11].

QKD, or Quantum Key Distribution, entails the transfer of quantum particles, usually photons, from a transmitter (Alice) to a receiver (Bob) [12]. The photons possess quantum information that may be encoded in several manners, often utilizing the polarization or phase of the photons. The security of Quantum Key Distribution (QKD) is based on the notion of quantum indeterminacy. This implies that any attempt by an eavesdropper (referred to as Eve) to intercept the quantum keys will inevitably disrupt the quantum states, therefore notifying Alice and Bob of the intrusion [13].

Quantum Key Distribution (QKD) is crucial for improving identity verification in quantum networks. QKD guarantees the generation of highly secure cryptographic keys [14], hence restricting access to sensitive data exclusively to authorized individuals. This procedure efficiently reduces the danger of identity fraud and illegal access, as the quantum keys are almost invulnerable to interception or decryption by malevolent individuals. QKD functions as a resilient basis for verifying identification, enhancing the security of quantum network communications.

Nevertheless, Quantum Key Distribution (QKD) is not exempt from its limits and practical issues. Implementation obstacles encompass the requirement for specialized hardware with the capacity to process quantum states, along with difficulties pertaining to the transmission of quantum signals across extensive distances. In addition, it should be noted that Quantum Key Distribution (QKD) does not offer a comprehensive solution for all aspects of identity authentication in quantum networks, such as user verification or access control. Although quantum key distribution (QKD) greatly improves security, it is only a single component in constructing a comprehensive and safe authentication system for quantum networks. However, its primary function of guaranteeing the secrecy and accuracy of cryptographic keys remains crucial to the overall security of quantum communication.

V. Protocol for Secure Quantum Identity Authentication

The Secured Quantum identification Authentication Protocol is an innovative method for verifying identification in quantum networks. The purpose of this protocol is to establish a security framework that utilizes the principles of quantum physics to authenticate identities at many layers. The system integrates quantum key distribution (QKD) techniques with traditional cryptography approaches to provide a secure and tamper-proof identity verification system.

The protocol consists of several essential elements, each fulfilling a vital function in the authentication process. The process starts by generating quantum keys by QKD, guaranteeing the creation of cryptographic keys in a manner that is secure against quantum attacks. Subsequently, these quantum keys are employed with traditional encryption methods to encrypt and safeguard user identification data while it is being sent [15].

The protocol utilizes many encryption methods, including symmetric and asymmetric cryptography, to protect user data and identification tokens. Quantum keys significantly bolster the security of conventional encryption systems, rendering it highly arduous for unauthorized entities to intercept or tamper with the authentication process [16].

The main objective of the protocol is to ensure safe verification of identification in quantum networks. This is accomplished by employing the concepts of quantum entanglement and the no-cloning theorem, which intrinsically safeguard quantum keys from unauthorized interception [17]. If an unauthorized person tries to intercept the quantum keys, it will unavoidably disrupt the quantum states, which will activate an alarm and prevent identity theft[18-23].

Moreover, the integration of quantum and conventional encryption methods provides an additional level of protection, rendering it highly difficult for malevolent individuals to breach user identities. The authentication procedure entails the transmission of encrypted identification tokens, which can only be deciphered by authorized parties with the matching quantum keys. This dual-layer encryption procedure guarantees that in the event of an interception of the encrypted material by an attacker, they would need both the quantum key and the understanding of conventional encryption techniques to decode it, which is almost impossible to do using computational methods.

VI. CONCLUSIONS

To summarize, the Secured Quantum Identity Authentication Protocol is a significant advancement in the pursuit of reliable identity verification in quantum networks. This protocol utilizes quantum key distribution in conjunction with classical encryption techniques to provide a multi-layered security architecture that effectively tackles the specific issues presented by the quantum domain. It provides both secure identity identification and establishes the groundwork for a future that is resistant to the risks presented by quantum computing, ensuring that data and communications remain unaffected.

The importance of this protocol cannot be emphasized enough, as it ensures the security and privacy of identity verification procedures within quantum networks, which are crucial for businesses spanning from banking and healthcare to national security. Furthermore, it emphasizes the significance of quantum security as we traverse the thrilling yet intricate realm of quantum technology. As quantum identity authentication and quantum communication continue to progress, it is becoming more apparent that quantum security will be crucial in protecting our digital world from new threats and weaknesses.

References

[1]Guha, T., Roy, S., & Chiribella, G. (2023). Quantum networks boosted by entanglement with a control system. Physical Review Research, 5(3), 033214.

[2] Badirova, A., Dabbaghi, S., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2023). A Survey on Identity and Access Management for Cross-Domain Dynamic Users: Issues, Solutions, and Challenges. IEEE Access.

[3] Paudel, H. P., Crawford, S. E., Lee, Y. L., Shugayev, R. A., Leuenberger, M. N., Syamlal, M., ... & Duan, Y. (2023). Quantum Communication Networks for Energy Applications: Review and Perspective. Advanced Quantum Technologies, 6(10), 2300096.

[4] Lu, Y., Sigov, A., Ratkin, L., Ivanov, L. A., & Zuo, M. (2023). Quantum computing and industrial information integration: A review. Journal of Industrial Information Integration, 100511.

[5] Mohanaprabhu, D., Monish Kanna, S. P., Jayasuriya, J., Lakshmanaprakash, S., Abirami, A., & Tyagi, A. K. (2024). Quantum Computation, Quantum Information, and Quantum Key Distribution. Automated Secure Computing for Next-Generation Systems, 345-366.

[6] Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2023). Peer-to-Peer User Identity Verification Time Optimization in IoT Blockchain Network. Sensors, 23(4), 2106.

[7] Yang, Z., Zolanvari, M., & Jain, R. (2023). A Survey of Important Issues in Quantum Computing and Communications. IEEE Communications Surveys & Tutorials.

[8] Li, Z., Xue, K., Li, J., Chen, L., Li, R., Wang, Z., ... & Lu, J. (2023). Entanglement-assisted quantum networks: Mechanics, enabling technologies, challenges, and research directions. IEEE Communications Surveys & Tutorials.

[9] Zhang, C. X., Wu, D., Cui, P. W., Ma, J. C., Wang, Y., & An, J. M. (2023). Research progress in quantum key distribution. Chinese Physics B.

[10] Ren, C., Yu, H., Yan, R., Xu, M., Shen, Y., Zhu, H., ... & Kwek, L. C. (2023). Towards Quantum Federated Learning. arXiv preprint arXiv:2306.09912.

[11] Alhayani, B. A., AlKawak, O. A., Mahajan, H. B., Ilhan, H., & Qasem, R. A. M. (2023). Design of quantum communication protocols in quantum cryptography. Wireless Personal Communications, 1-18.

[12] SOVIANY, S., & GHEORGHE, C. G. The QKD (Quantum Key Distribution) Application in Cyber Security.

[13] Alhayani, B. A., AlKawak, O. A., Mahajan, H. B., Ilhan, H., & Qasem, R. A. M. (2023). Design of quantum communication protocols in quantum cryptography. Wireless Personal Communications, 1-18.

[14] Bajrić, S. (2023). Enabling Secure and Trustworthy Quantum Networks: Current State-of-the-Art, Key Challenges, and Potential Solutions. IEEE Access, 11, 128801-128809.

[15] Rao, B. D., & Jayaraman, R. (2023). A novel quantum identity authentication protocol without entanglement and preserving pre-shared key information. Quantum Information Processing, 22(2), 92.

[16] Chen, G., Wang, Y., Jian, L., Zhou, Y., Liu, S., Luo, J., & Yang, K. (2023). Quantum identity authentication protocol based on flexible quantum homomorphic encryption with qubit rotation. Journal of Applied Physics, 133(6).

[17] Azahari, N. S. B., Harun, N. Z. B., & Zulkarnain, Z. B. A. (2023). Quantum identity authentication for non-entanglement multiparty communication: A review, state of art and future directions. ICT Express.

[18] Chaudhary, P., Gupta, B., & Singh, A. K. (2022). Implementing attack detection system using filter-based feature selection methods for fog-enabled IoT networks. Telecommunication Systems, 81(1), 23-39.

[19] Colace, F., Guida, C. G., Gupta, B., Lorusso, A., Marongiu, F., & Santaniello, D. (2022, August). A BIM-based approach for decision support system in smart buildings. In Proceedings of Seventh International Congress on Information and Communication Technology: ICICT 2022, London, Volume 1 (pp. 471-481). Singapore: Springer Nature Singapore.

[20] Gupta, B. B., & Sheng, Q. Z. (Eds.). (2019). Machine learning for computer and cyber security: principle, algorithms, and practices. CRC Press.

[21] Bhushan, K., & Gupta, B. B. (2017). Security challenges in cloud computing: state-of-art. International Journal of Big Data Intelligence, 4(2), 81-107.

[22] Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. International Journal on Semantic Web and Information Systems (IJSWIS), 18(1), 1-43.

[23] Gupta, B. B., Perez, G. M., Agrawal, D. P., & Gupta, D. (2020). Handbook of computer networks and cyber security. Springer, 10, 978-3.