Review of Quantum Cybersecurity and Efficient resource sharing for Mobile Edge Cloud Computing

*Note: Sub-titles are not captured in Xplore and should not be used

Shashwat Tiwari
Computer Science Engineering
Shiv Nadar Institute of Eminence
2010111038

***Abstract*—This paper gives us a brief overlook of the threats, risks, and opportunities of quantum cybersecurity, efficient computing resource sharing for mobile edge-cloud computing networks and edge-computing visions and challenges.**

***Index Terms*—component, formatting, style, styling, insert**

I. Review of Quantum Cybersecurity: Threats, Risks and Opportunities

A. Introduction

The increasing digitization of sensitive data in databases highlights the importance of cybersecurity in protecting against cyber threats. As cyber-attacks become more frequent, the field of cybersecurity is looking to embrace futuristic technologies like AI, Quantum Computing, Blockchain, and Data Science. However, the potential risks and opportunities of Quantum Computing on cybersecurity must be investigated to prevent current cybersecurity infrastructure from becoming obsolete. This paper aims to study the intersection between Quantum Computing and Cybersecurity and explore ways to enhance Quantum Computing cybersecurity for concerned stakeholders.

B. Paper Organization

This section outlines the organization of the paper and its various sections. I. Introduction This section introduces the paper and its focus on quantum cybersecurity. II. Research Design and Methodology This section explains the research design and methodology used for the paper, including research questions on both positive and negative aspects of quantum cybersecurity. III. Overview of Quantum Computing and Cybersecurity This section provides a thorough overview of quantum computing and cybersecurity. IV. Related Studies This section reviews 20 primary studies on quantum computing and cybersecurity and synthesizes the findings, approaches, and considerations. V. Findings and Future Research Directions This section discusses the findings and challenges identified from the review and provides guidelines for future research in this field. VI. Conclusion This section concludes the paper and summarizes its main contributions.

Identify applicable funding agency here. If none, delete this.

C. Research Design and Methodology

1) Research Goals: This study aims to address three key research questions related to the intersection of quantum computing and cybersecurity. The first research question seeks to define quantum computing and how it can intersect with cybersecurity. The second research question evaluates quantum cybersecurity's potential opportunities and risks. Finally, the third research question explores the improvements that can be carried out in quantum cybersecurity. The authors recognise the threat posed by the development of quantum computing to cybersecurity and aim to provide insights that can improve the understanding of this intersection.

2) Study Selection: To identify research papers relevant to the study, the authors implemented a search process using various scientific databases. They prepared potential search strings containing keywords related to the study topic, including "Quantum Cybersecurity," "Quantum Computing for Cybersecurity," "Cybersecurity for Quantum Computing," "Quantum-enabled Cybersecurity," and "Post-Quantum Cybersecurity." The authors then applied specific search strings using the selected keywords and the title of the papers during the analysis. The search was conducted on March 01st, 2022, and included all studies published up to that date. The scientific databases used for procuring these papers included Google Scholar, IEEE Xplore Digital Library, ScienceDirect, ACM Digital Library, SpringerLink, and arXiv e-Print Archive. The authors used a systematic literature review process and depicted the attrition of the literature through processing in Fig.

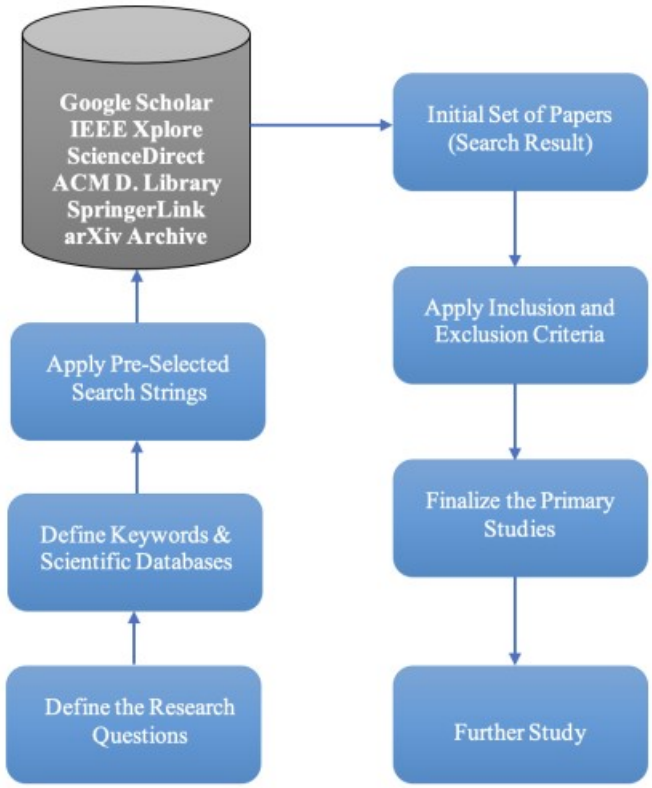

Fig. 1. Attrition of Systematic Literature thorough processing

3) Results of the Studies: After completing the initial search, a total of 354 research papers were identified. However, the authors applied the inclusion and exclusion criteria to ensure that only relevant papers were included in the study. This process excluded 329 papers, leaving 25 papers for further review. The authors then conducted a full-text review of these 25 papers and excluded four more papers that did not meet the inclusion criteria. Thus, a total of 21 papers were finally included in the study. The authors used a PRISMA flow diagram to depict the selection process presented in Fig.

D. Related Studies

The text discusses a few research papers on post-quantum cryptography. Some of the papers that have been mentioned are as follows: One paper proposes five types of post-quantum cryptosystems for blockchain technology. The paper suggests that rapid advancement in quantum computing using Grover's and Shor's algorithms puts hash functions and public-key cryptography at risk. The proposed cryptosystems are resilient to quantum threats and can be used for encryption and digital signatures in blockchain. Another paper suggests lattice-driven cryptographic techniques for quantum resistance security models in the Internet of Things (IoT). The paper analyzes the vulnerabilities of current IoT architecture and implementation and proposes improvements to protect IoT in the post-quantum era. A third paper proposes KeyShield, a scalable and quantum-safe key management scheme that outperforms state-of-the-art schemes in quantum-resistance, computation cost, message overhead, storage cost, and rekeying delay. The paper provides mathematical analysis and proofs to support the proposed scheme.

E. Conclusion

The emergence of quantum computing can significantly impact cybersecurity as it can be used both as a threat and a solution. The study reviewed the current quantum computing and cybersecurity state-of-the-art and identified proposed approaches. Quantum computing can be used to enhance cybersecurity, but it also poses threats to cybersecurity. The review highlights the need for further research in this emerging field and provides insights into future research directions for quantum and cybersecurity practitioners and researchers.

II. Efficient Computing Resource Sharing for Mobile Edge-Cloud Computing Networks

A. Introduction

The demand for mobile applications has brought challenges to designing mobile devices with limited hardware capabilities. The cloud and edge can provide computing services to address this challenge, but designing an efficient cooperative edge-cloud network and business model is necessary for the future. Our previous work proposed an efficient wholesale and buyback scheme for managing computing resources in mobile edge-cloud computing networks to maximise profitability and QoS. However, the scheme did not consider the impact of cloud operation costs and computing requirements on wholesale prices. Therefore, we propose a joint pricing scheme for cloud computing resources to determine optimal computing resources for both the MEC and cloud. The scheme emphasizes the importance of collaboration between the cloud and edge servers and highlights the potential benefits for both entities. The rest of the paper introduces related works, proposes a framework for mobile edge-cloud computing networks, and formulates computing resource management problems. The paper concludes with simulations demonstrating the efficiency of the proposed algorithm.

B. Related Works

The related works discussed in this paper can be categorised into two perspectives: system design and system optimisation to enhance MEC systems. For instance, a MEC-based object detection architecture was proposed for real-time surveillance applications. An air-ground integrated mobile edge network (AGMEN) using UAVs was proposed to improve the edge's communication, caching, and computing network. On the other hand, from a system optimisation perspective, researchers have proposed schemes to optimise different aspects of MEC systems, such as energy consumption, workload allocation, and resource allocation. For example, an energy-efficient computing offloading management scheme was proposed to reduce the energy consumption of mobile devices. In contrast, an optimal workload allocation scheme was proposed to balance power consumption and transmission delay. Moreover, a joint radio and computational resource allocation scheme were designed to enhance system performance and improve user

satisfaction. In addition to these approaches, some studies proposed heuristic solutions to address system design and optimisation problems.

C. System model and problem formulation

The problem formulation in this system model can be described as a resource allocation problem. The goal is to optimize the utilization of computing resources between the MEC servers and the cloud servers. The objective is to maximize the system's overall profit while ensuring the computing tasks' QoS requirements. To achieve this objective, the system must determine the optimal allocation of computing resources between the MEC servers and the cloud servers, considering the current computing requirements, available computing resources, and the costs of computing resource wholesale and buyback. The problem is further complicated by the time-sensitive nature of the computing tasks and the need to ensure QoS. The resource allocation problem can be mathematically formulated as an optimization problem, where the objective function is to maximize the overall profit of the system, subject to constraints such as the QoS requirements, resource availability, and computing resource costs. The optimization problem can be solved using various optimization techniques, such as linear programming, dynamic programming, or heuristic algorithms.

1) Operation Model of Mobile Edge Computing (MEC): The MEC server's computing resources are divided into two parts, one reserved for local computation tasks and the other wholesaled to the cloud for flexible computation tasks. Communication delay between MEC servers and the cloud is negligible due to wired connections and local processing.

2) Operation Model of Cloud Computing: Cloud computing resources are available from cloud servers and MEC servers, managed by the cloud. The wholesale and buyback scheme of MEC servers affects the availability of computing resources from MEC servers.

D. Profit Model of MEC and Cloud Computing

The profit of MEC servers includes operation cost, income from local processing, income from wholesaling computing resources to the cloud, and cost for buying back computing resources. The total profit depends on the wholesaled and buyback scheme of the MEC server. The profit of the cloud includes processing computing tasks, local operation cost, and trading computing resources with MEC servers. The cloud needs to balance operation costs and QoS penalty.

E. Wholesale and Buyback with Profit

The MEC and cloud have different profit objectives but can share computing resources with profit transfers. The MEC aims to maximize profit by providing computing services and wholesaling computing resources, while the cloud aims to provide better computing services and reduce operation costs. MEC servers determine their wholesale and buyback scheme, while the cloud determines the wholesale price and manages cloud computing resources. These problems are coupled by profit transfers, and optimal pricing and resource management are required to maximize the profits of both MEC and cloud.

F. Conclusion

This paper proposed a framework for efficient resource sharing between the MEC and the cloud to improve their profitability. Two cases were considered: social welfare maximization and respective profit maximization. For the first case, it was proved that the social welfare only depends on the cloud computing resources and the concavity of the social welfare maximization problem. For the second case, an optimal pricing and cloud computing resource management were designed to maximize the total profit. Numerical evaluations showed that the proposed algorithms can maximize the social welfare and the respective profits of the MEC and the cloud separately. However, the assumptions made in this paper are that all MEC servers have the same computing resources and all computing tasks have similar QoS requirements.

ACKNOWLEDGMENT

I would like to express my sincere gratitude to Shiv Nadar Institute of Eminence for providing me with the opportunity to work on this research paper. The experience of conducting original research and contributing to the academic discourse has been invaluable in shaping my academic and professional goals.

I would also like to extend my heartfelt thanks to Professor Sonia Khetarpaul, whose guidance, support, and encouragement made this project possible. Her expertise, patience, and dedication have inspired me to pursue further research in this field.

In addition, I would like to acknowledge the contributions of my fellow classmates and colleagues, whose feedback and insights were instrumental in shaping this work. I am grateful for their intellectual generosity and collegial spirit.

Finally, I would like to thank my family and friends for their unwavering support and encouragement throughout this process. Their belief in me and my abilities has been a constant source of motivation and inspiration.

REFERENCES

[1] M. J. Hossain Faruk, S. Tahora, M. Tasnim, H. Shahriar and N. Sakib, "A Review of Quantum Cybersecurity: Threats, Risks and Opportunities," 2022 1st International Conference on AI in Cybersecurity (ICAIC), Victoria, TX, USA, 2022, pp. 1-8, doi: 10.1109/ICAIC53980.2022.9896970.

[2] Y. Zhang, X. Lan, J. Ren and L. Cai, "Efficient Computing Resource Sharing for Mobile Edge-Cloud Computing Networks," in IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1227-1240, June 2020, doi: 10.1109/TNET.2020.2979807.