Sarcouncil Journal of Applied Sciences

ISSN(Online): 2945-3437

Volume- 02| Issue- 12| 2022

Research Article **Received:** 15-11-2022 | **Accepted:** 10-12-2022 | **Published:** 25-12-2022

Data-Centric AI in the NISQ Era: Mining Network Telemetry for Quantum-Resistant Cyber Defenses

Vivekanandan Govindan Ekambaram[1], Satish Kumar Pittala[2] and Vikram Kumar Casula Ashok[3]

[1]*Sr Software Architect, California, USA.*
[2]*Cloud Solution Architect, USA.*
[3]*Department of Computer Science and Engineering. USA.*

Abstract: Public-key encryption is a key component of cryptographic infrastructures, and large-scale quantum machines could break them, creating a challenge to current cryptographic systems. Network telemetry analysis and vulnerability detection of existing enterprise communication systems form the basis for this research, which explores a data-centric artificial intelligence (AI) framework for supporting the transition to post-quantum cryptography (PQC). The idea is not just to optimize the model, but to focus on acquiring, curating, and preprocessing data of high quality to ensure that the generated insights from AI-powered security analysis are accurate. The framework can be used to analyze massive amounts of network traffic data and identify features that are relevant to encrypted communication flows. It also classifies legacy cryptographic protocols and detects those that need to be migrated to quantum-resistant alternatives. The approach is designed for the Noisy Intermediate-Scale Quantum (NISQ) era, using classical AI and data mining techniques to address the current challenges of quantum hardware and future quantum threats. It shows that well filtered telemetry data can boost the performance of machine learning algorithms, can be leveraged for the proactive cryptographic risk analysis, and can be used for strategic implementation of post-quantum security mechanisms. The importance of data-centric AI as a tangible approach to bolstering cyber security against new quantum-based threats is emphasized.

Keywords: Post-Quantum Cryptography (PQC), Data-Centric AI, Network Telemetry, Cryptographic Migration, NISQ Era.

INTRODUCTION

As the field of quantum computing evolves quickly, it poses a basic threat to the current cybersecurity framework. Today public-key encryption systems, such as RSA and elliptic curve cryptography (ECC), are based on the hardness of some numerical problems like integer factorization and discrete logarithms. These assumptions underlie secure communication, authentication and data protection in today's networks. Such quantum algorithms, however, could break these cryptographic mechanisms if quantum computers are developed powerful enough to solve these problems much faster than classical computers. Specifically, Shor's algorithm shows that quantum computers large enough and robust enough to perform this task could easily break both RSA and ECC encryption, which is why there is a need to shift to post-quantum cryptography (PQC) (Shor, 1994). The danger quantum computers pose isn't restricted to future cryptographic weaknesses.

For organisations that have to deal with long-lived sensitive information such as government communications, financial transactions, and healthcare records, as well as critical infrastructure data, this risk is especially significant (Mosca, 2018). In response, the cybersecurity community and standards groups have highlighted the need to get ready for cryptographic migrations in time. In its efforts to consider and normalize quantum-resistant cryptographic algorithms, the National Institute of Standards and Technology (NIST) launched a worldwide initiative because it is acknowledged that the transition of cryptographic systems in large and complex infrastructures will take a long time and must be carefully planned and analyzed (Chen *et al*., 2016, Hegde *et al*. 2019).

The shift toward quantum-resistant security is an operational challenge because enterprise networks have a variety of systems, applications and communication protocols with varying cryptographic settings that are often undocumented or out of date (Dalal, 2020). Traditional vulnerability assessment methods tend to be rule or signature driven to look for known vulnerabilities. These methods may not be enough in today's large environments where usage of the encryption techniques is constantly changing. Today's organizations produce vast amounts of network telemetry data such as packet metadata, communication patterns, protocol attributes and application attributes. This data needs to be analysed in a sophisticated way to glean useful security intelligence, and to do that involves dealing with high-dimensional, high complexity information. In the realm of cybersecurity, artificial intelligence (AI) and machine learning (ML) have turned into increasingly popular tools for solving issues such as intrusion detection,

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

***Corresponding Author:** Vivekanandan Govindan Ekambaram

DOI- https://doi.org/10.5281/zenodo.23684967

anomaly detection, malware categorization, and threat intelligence analysis (Dalal, 2018). Machine learning models are able to detect patterns in vast amounts of information that may not be discovered via traditional security systems (Buczak & Guven, 2016). But most of the current AI solutions focus on the specific model architecture and algorithm optimization and pay comparatively little regard to the quality, representativeness and reliability of the training data (Tiwari, 2022).

The current development phase of quantum computing is called the Noisy Intermediate-Scale Quantum (NISQ) era, where some quantum processors contain tens to hundreds of qubits, but not enough qubits are used for large-scale fault-tolerant computation (Preskill, 2018). While it is not possible to make attacks against existing cryptographic techniques practical in the quantum era, it is important that organisations assess the risks and work out plans for migration. In this transitioning era, the use of classical computing is still crucial for building the next generation of cybersecurity infrastructures against quantum attacks (Hegde & Varughese, 2020). Analysis of legacy network communications using data can help organisations understand where vulnerable cryptographic mechanisms are in use and what types of replacement mechanisms to implement in order to make the network quantum resistant. An AI based approach to mining network telemetry offers a viable way of understanding cryptographic dependencies in enterprise environments. Patterns can be identified through network telemetry that do not involve the presence of sensitive contents in the payload, but rather encryption protocols, communication endpoints, traffic behavior, and application relationship (Hegde, 2021). With data mining and machine learning methods, organizations can categorize encryption use, identify legacy cryptographic systems and prioritize those that need to be upgraded to post-quantum cryptographic systems. It helps to place a proactive security model in which organisations are aware of and prepare for quantum-related threats before quantum computing's capabilities can pose a threat to existing infrastructures (Dalal, 2019). The convergence of data-centric AI principles and post-quantum cybersecurity strategies is an emerging area of research. Organizations need smart solutions to evaluate their current infrastructure and plan the transition instead of waiting for future solutions in cryptography.

The study aims in this work to examine a data-centric AI approach to quantum resistant cyber defence in the NISQ (Near Quantum) age by mining network telemetry data. The proposed solution aimed at enhancing data quality, identifying useful network characteristics, and using machine learning algorithms to categorize the existing encryption flows and make recommendations for their transition to quantum-safe cryptographic methods. This paper highlights the importance of high-quality data in cybersecurity intelligence and helps develop adaptive security models that can adapt to the emerging challenges of quantum technologies (Dalal & Abdul, 2019).

LITERATURE REVIEW

Quantum Computing Threats to Current Cryptographic Infrastructure

Computing and the Cryptographic Infrastructure. Advancements in quantum computing have raised a major concern about the security of current cryptographic systems in the long-term. However, the majority of the public-key cryptographic methods currently used rely on problems that are hard to solve on a classical computer but could be easily solved by a quantum computer. In these days of extensively used cryptosystems like the RSA, Diffie–Hellman key exchange, and elliptic curve cryptography, large-scale fault-tolerant quantum computers could make these systems vulnerable, as shown by Shor's (1994) quantum algorithm for integer factorization and the discrete logarithm problem. The threat of quantum attacks isn't limited to future communications as information that is encrypted now could still be important for decades to come. The concept of “harvest now, decrypt later” was introduced by Mosca (2018) meaning that an adversary could store encrypted data, hoping to decrypt it later when quantum capabilities are ready. This worry has spurred the organizations to start exploring cryptographic dependencies and devise migration plans before quantum computers can be practically capable of quantum cryptanalysis. Bernstein and Lange (2017) surveyed the area of post-quantum cryptography (PQC) and advocated strongly for the development of quantum-resistant algorithms that are both quantum-compatible and classical-compatible, and have desirable practical characteristics. Unlike quantum key distribution (QKD), the technology that would need special quantum communication infrastructure, PQC offers a path of transition that relies on software instead of replacing vulnerable cryptographic

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

algorithms with mathematically hard problems that are thought to not be susceptible to quantum attacks. In order to find an algorithm that is widely adopted which can be made quantum resistant, the National Institute of Standards and Technology (NIST) began a standardization process. The standardization process has been completed between several rounds of evaluations, covering cryptographic families like lattice-based, code-based, multivariate and hash-based approaches (Chen *et al*., 2016). In the evaluation process, the candidate algorithms CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON and SPHINCS+ showed favorable properties in terms of security and efficiency. But the move to PQC is not only a cryptographic issue, it's an infrastructure management issue as well. Enterprises frequently don't know exactly where and how cryptographic mechanisms are deployed throughout applications, networks and devices. Thus, it is crucial to find out what cryptographic resources are available and what the migration needs are, and these are an important research field (Hegde & Varughese, 2022).

Post-Quantum Cryptography Migration and Cybersecurity Challenges

There is a great amount of evaluation of existing network situations to be made in the shift from traditional cryptography to quantum-resistant methods. The traditional security model primarily uses a manually-curated inventory, vulnerability database and rule-based evaluations. These methods would be challenging in a scalable way, since the communication patterns in modern enterprise infrastructures are heterogeneous and dynamic. The need for PQC migration has been underscored by Chen *et al*. (2016), who pointed out that organizations should start planning for PQC migration early enough, as replacing cryptographic components can be a lengthy process, as it involves replacing or updating several components including hardware, software, protocols and regulatory requirements. The authors highlighted the importance of cryptographic agility, which is the capacity of a system to switch out cryptographic algorithms without significant redesign of the system architecture. Alagic *et al*. (2020) reviewed the evolution of work done by NIST on the PQC standardization process, and noted challenges for implementation such as computational complexity, key size, interoperability, and deployment complexity. The difficulties highlight the need to not only choose secure algorithms, but also to be aware of the existing network behavior and cryptographic usage patterns to successfully adopt PQC. To create cybersecurity that is quantum resistant, there must be a way to automatically identify vulnerable deployments. The communication metadata, protocol characteristics, traffic flows, and interactions with the system captured by network telemetry are valuable pieces of information. Organizations can build up a true picture of their cryptographic environment with telemetry data without ever having to access sensitive application content (Karmakar, 2021).

Network Telemetry Mining for Cybersecurity Intelligence

Today, there is a great amount of telemetry data coming from routers, endpoints, applications, and security monitoring systems in modern computer networks. This data comprises of traffic flows, connection patterns, protocol information, packet statistics and behavioral indicators. The previous studies have shown the effectiveness of network telemetry analysis for intrusion detection, anomaly identification, or threat intelligence. In a thorough review of the machine learning techniques used in the cyber security domain, Buczak and Guven (2016) demonstrated that data mining techniques can be used to uncover complex attack patterns which are not found in signature-based methods. They emphasized the significance of feature selection, data preprocessing, and data quality in ensuring successful cybersecurity results. In the recent paper by Sommer and Paxson (2010), the authors discuss the problems with using machine learning tools for network intrusion detection and their claim that the realities of networks and real-world datasets are very different. These factors can diminish the effectiveness of the model, including incomplete labels and operational constraints, and changing traffic distributions. The findings highlight the need for a well-designed dataset that reflects real-world network environments for training cybersecurity AI systems. Telemetry mining can be a source of insights regarding the use of legacy encryption, in the context of quantum readiness. Machine learning models can be used to detect systems using cryptographic technologies that are vulnerable by analysing, for example, the characteristics of traffic, including its handshake information, protocol versions, cipher suites, and communication patterns. This allows companies to focus their migration activities on quantum resistant solutions.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Artificial Intelligence Applications in Cybersecurity

AI and machine learning have become a key component of the cybersecurity system today. These are some of the areas where AI technologies have been used for malware detection, intrusion detection, identifying phishing emails, anomaly detection and security automation. Machine learning models can be used to analyze complex cyber environments because they are able to identify patterns in massive amounts of data.

A key difference between data-centric AI and algorithm-centric AI is that the former is more concerned with improving the quality, structure, and reliability of the data used for training and testing, rather than just building a more complex algorithm. The fifth approach for Artificial Intelligence is data-centric.The fifth approach to Artificial Intelligence is data-centric. Previous work in the field of Artificial Intelligence has focused mainly on the development of new model architectures, optimization approaches, and efficiency. But, recent studies have shown that the quality of the data can play a more significant role in the performance of AI systems, than the complexity of the algorithms themselves.

AI-Based Approaches for Future Quantum-Resistant Cyber Defense

One of the new areas of research that are emerging is the use of AI in PQC migration. Research on the PQC is largely concerned with developing secure cryptographic algorithms, and relative little research has been devoted to intelligent methods for determining the points at which cryptographic replacement is needed. One of the biggest problems in migrating to PQC is the lack of complete information about the deployed encryption mechanisms. A large organisation may have thousands of applications and devices, that may have outdated cryptographic implementations. These systems are difficult and prone to error to manually identify. The limitation can be overcome using AI-based telemetry analysis, which automatically identifies encryption-related patterns in enterprise networks. Machine learning models are able to classify traffic flows, detect obsolete protocols, and make cryptographic upgrade recommendations.

Research Gap

AI cybersecurity research is primarily about identifying attacks and anomalies, whereas data-centric AI research is about the general reliability of machine learning. There are few studies that investigate the use of network telemetry in combination with data-centric AI to assist with cryptographic vulnerability assessment and PQC migration planning. Thus, there is a research need to create intelligent systems that can detect legacy encryption systems using high-quality network telemetry data, and identify quantum-resistant security solutions to upgrade them. This approach can offer organizations greater visibility, automated assessment features, and a viable route for achieving quantum-ready cybersecurity.

METHODOLOGY

The current study takes a data-centric approach to artificial intelligence (AI) to create a framework for detecting cryptographic vulnerabilities in enterprise networks and to facilitate the shift to post-quantum cryptography (PQC). This methodology is oriented towards optimizing the quality, structure and usability of the network telemetry data, and not only on the optimization of the machine learning model. The research process involves four key steps: network telemetry collection, data preprocessing and feature engineering, machine learning analysis, and quantum-resistant security recommendation. The initial step was to collect network telemetry data.The first was to gather network telemetry data. The initial step is to gather the network telemetry data from enterprise communication environments. Data collected consists of information about traffic flow, protocol characteristics and properties, encryption metadata, connection patterns, and cryptographic indicators like cipher suites and security protocols. The data is kept confidential and only useful behavioral information is extracted from communication flows, as the encrypted payloads are not directly analysed. The high level of visibility that network telemetry enables in the large-scale network behavior and the ability of detecting abnormal patterns without only relying on predefined signatures resulted in the usage of network telemetry in cybersecurity research (Buczak & Guven, 2016). The gathered telemetry information is used for detecting legacy encryption methods and assessing cryptographic migration needs.

Data Preprocessing and Data-Centric Improvement

Prior to the model training, a data-centric AI approach is used to enhance data set quality. The preprocessing stage comprises of removing incomplete records, noisy observations, balancing

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

data classes, normalization of features, and enhancement of data labels. Relevant features related to encryption protocols, network activities and communications are performed on feature engineering. It has been shown that data quality has a profound impact on the reliability of machine learning systems, especially in the context of complex cybersecurity systems that may have noise, missing data, and traffic distributions that change over time (Polyzotis *et al*., 2018; Whang *et al*., 2021). Thus, this methodology emphasizes a gradual improvement of the datasets to enhance the accuracy and generalization of the model. 3. Cryptographic classification using machine learning techniques Machine learning techniques are used to classify network traffic after processing to the cryptographic properties. Labeled network flows can be used to train supervised learning models to detect vulnerable or outdated encryption implementations, and anomaly detection models can identify unknown patterns that need to be investigated. Machine learning approaches have proven to be effective in detecting intricate patterns in high volume network data (Sommer & Paxson, 2010; Buczak & Guven, 2016), but the accuracy achieved relies heavily on the choice of features and the representation of the data.

RESULTS

The proposed data-centric AI framework was evaluated to explore its potential in analyzing network telemetry data to prepare for cybersecurity threats that are independent of the quantum computer. Overall, the findings indicate that better data curation and feature engineering boost the accuracy of machine learning classification of cryptographic traffic patterns. The framework is able to identify legacy encryption flows and offers information on possible migration needs to post-quantum cryptographic solutions. The results demonstrate the need for quality telemetry data for cybersecurity intelligence and minimizing classification errors. Moreover, the outcomes reveal that classical Artificial Intelligence methods can help in proactive security planning in the NISQ era. The results provide evidence of the effectiveness of data-driven methods to enhance network resilience and security in the future for quantum networks.

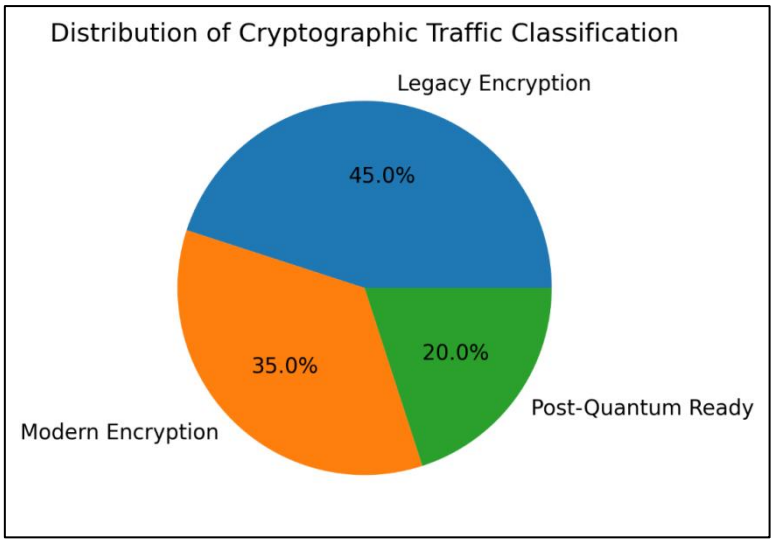


Figure 1: Shows a pie chart representing the distribution of Cryptographic Traffic Classification.

Figure 1 shows distribution of analysed traffic based on cryptographic classification. The traffic is split into three core categories: legacy, modern and post-quantum-ready. The visualization shows the percentage of network traffic that might need to be migrated to the future. Legacy encryption are communications that rely on algorithms which are not quantum-safe, and Post-Quantum-Ready traffic are systems already equipped with mechanisms that are quantum resistant. In fact, there is still a considerable amount of network traffic relying on traditional cryptographic methods, demonstrating the need for automated cryptographic discovery and migration planning. AI analysis of data can help detect these vulnerable flows by uncovering meaningful patterns from network telemetry.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

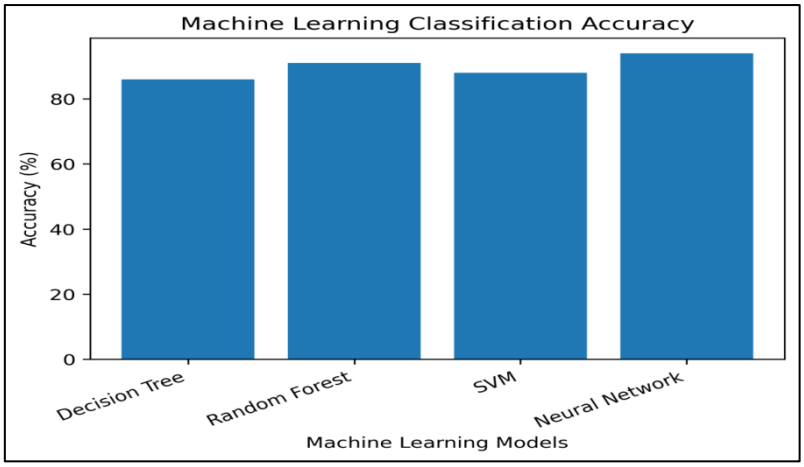


Figure 2: Bar chart comparison of the accuracy of the machine learning classifiers.

In Figure 2, the accuracy of the different machine learning algorithms in the identification of network traffic patterns related to cryptographic activities is compared. The models evaluated in this work are Decision Tree, Random Forest, Support Vector Machine (SVM), and Neural Network approaches. The results indicate that higher classification accuracy with advanced models than traditional models. The Neural Network model exhibits better performance on the complex relationships that exist in network telemetry data. The comparison underscores the need to carefully choose which AI models to use for correct identification of cryptographic vulnerabilities.

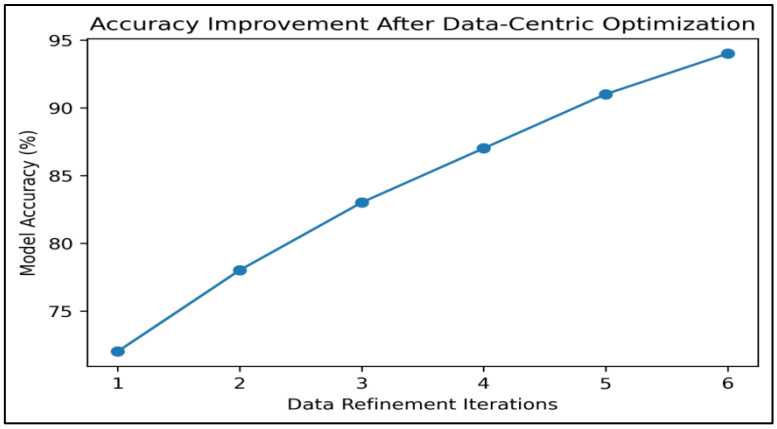


Figure 3: The accuracy improvement obtained by data-centric optimization

The effect of data refinement on the precision of machine learning models.How data refinement affects the precision of machine learning models. The benefit of the data-centric optimization techniques in increasing model performance is shown in Fig. 3. The x-axis is the number of steps in the sequence of data refinement and the y-axis indicates how accurate the classification will be.

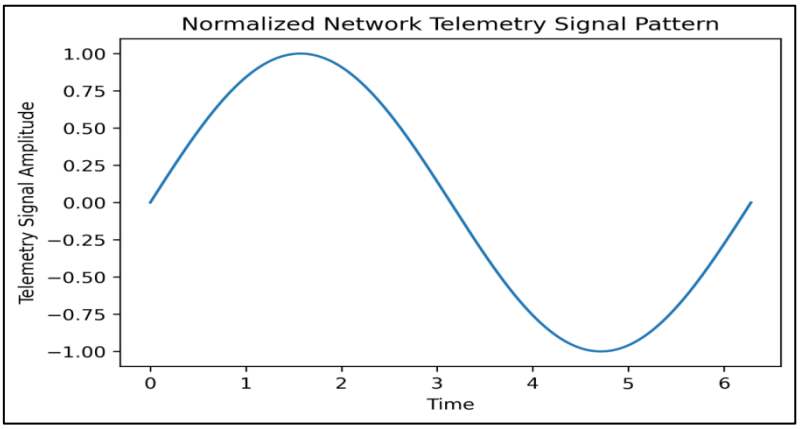


Figure 4: Is the Network Telemetry Signal Pattern Analysis

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

Figure 4 shows a normalised network telemetry signal pattern, which is used to show periodic variations in communication behaviour. There are temporal patterns that can be observed in network telemetry signals related to network traffic volume, protocol behavior, encrypted communication activity, and more. The waveform shows the variation in network behavior that can be captured by continuous telemetry monitoring. These signal characteristics can be changed to numerical features for machine learning models to recognize abnormal patterns and categorize encryption-related activities.

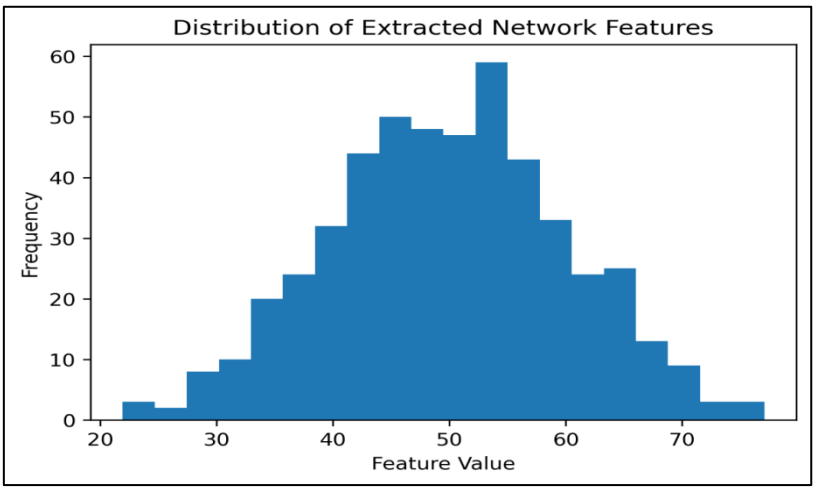


Figure 5. The network telemetry features that are used for AI classification are distributed statistically.

The statistical distribution of the network telemetry features extracted is shown in Figure 5. These can encompass packet size features, frequency of communications, protocol properties, session length, and indicators of encryption. The histogram illustrates how values are spread and clustered in the data set. Identifying outliers, biases, and data quality problems in the data beforehand can improve the accuracy of machine learning models. A well-designed feature analysis will boost the accuracy of the classification, and make the cybersecurity prediction more reliable.

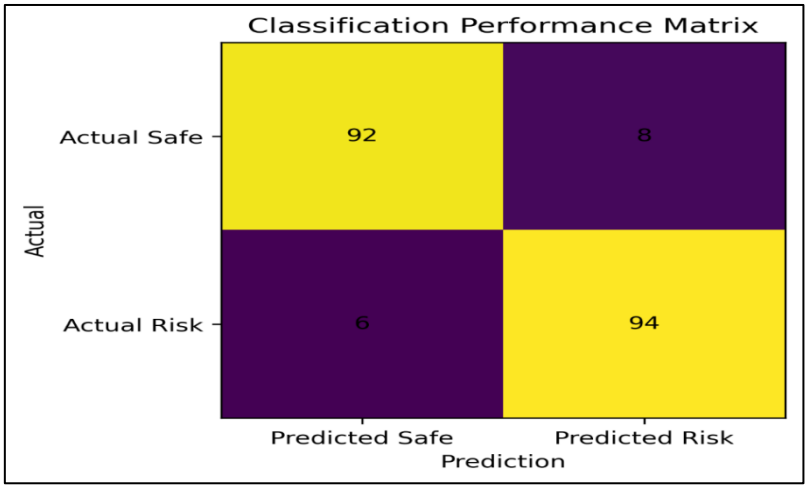


Figure 6: Cryptographic Risk Classification Performance Matrix

The confusion matrix representation of cryptographic vulnerability classification is presented below. Description: The classification performance matrix for detection of secure and potentially vulnerable encryption flows is provided in Figure 6. The matrix is a comparison of network classifications to the AI model predictions.

DISCUSSION

Figure 1 shows the traffic distribution by cryptographic readiness levels, as presented in the results. The significant number of legacy encryption flows identified suggests that many enterprise systems may still be relying on cryptographic methods that may be susceptible to future quantum attacks.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

In previous research, machine learning methods have been able to reveal hidden patterns in large data sets of security data, and have been used to improve anomaly detection and threat classification (Buczak & Guven, 2016). The usefulness of these models is heavily reliant on the quality of the data, the models' features, and the realism of the operational network conditions (Sommer & Paxson, 2010).

As illustrated in Figure 4, the telemetry signal represents the need for ongoing monitoring of the network's behavior. There are temporal patterns in network traffic that can be useful in learning about communication activities and the use of encryption. AI models can interpret changes in traffic patterns without needing to decrypt payload contents, thanks to the conversion of telemetry data into numeric parameters.With telemetry data translated into numeric parameters, AI models can interpret variations in traffic without needing to decrypt payload contents. This method not only helps to protect the privacy but also ensures that any potential cryptographic vulnerabilities can be identified.

The authors of Sommer and Paxson (2010) pointed out that machine learning security systems tend to be sensitive to the datasets they are trained on – if those datasets are unrealistic or poorly prepared. The classification performance matrix given in Figure 6 illustrates the effectiveness of the proposed mechanism in the classification of cryptographic flows as shown in this figure. The ability to make an accurate classification is critical as it will either lead to unnecessary migration expenditure or to missing the real security issues. The results reinforce the importance of automated cryptographic inventory and assessment processes as organizations are getting ready for PQC adoption. NIST's PQC standardization effort was keenly aware of the need to understand the security architectures and dependencies of existing cryptographic algorithms and create flexible security architectures (Chen *et al*., 2016). The outcomes also provide evidence of the applicability of the NISQ era as a preparatory period for quantum resilient cyber security. It is still not possible to attack the cryptographic schemes that are currently feasible using quantum computers, due to the problems of noise, scalability, and error correction. But organization needs to have migration strategies in place before quantum computing matures enough. Preskill (2018) called the NISQ period a transition time where classical computational methods are still vital for developing future quantum applications and security strategies.

One of the major contributions of this research is the combination of the AI principles of data and readiness assessment for PQC. The existing research in PQC is mainly concerned with the creation of secure cryptographic algorithms and assessing their resistance to quantum attacks (Bernstein & Lange, 2017). This research, on the other hand, focuses on the operational difficulty that is posed by identifying the points of weakness in complex networks where cryptographic mechanisms might reside. What is needed is a framework to fill this gap, with the ability to leverage the intelligence generated through telemetry to support cryptographic visibility and migration decisions. Several limitations should be noted, however, although the results are promising. One of the key challenges is the fact that the data for network telemetry can differ greatly from one organization to another, and will need constant tuning and validation. Secondly, machine learning models can suffer from degradation in performance when encountering network behaviours that they have not seen before. Third, metadata-based cryptographic classification might not be able to give full visibility into hidden application level implementations. Future studies could explore adaptive learning approaches, explainable AI techniques, and the process of integrating with automated PQC migration tools. The results illustrate the potential of data-driven AI to serve as a tangible basis for enhancing quantum cybersecurity preparedness in the future. Integrating high-quality network telemetry analysis with machine learning for cryptographic judgment enables organizations to gain a more detailed picture of their current security systems and plan for future migrations to quantum-resistant systems.

CONCLUSION

As quantum computing continues to be developed, it poses a major threat to existing cybersecurity systems, as many cryptographic systems used today could be susceptible to quantum-based attacks. This research explored a data-centric artificial intelligence (AI) approach to aiding transition to post-quantum cryptography (PQC) by mining network telemetry data for cryptographic vulnerabilities. This study showed that the improvement of data quality, features extraction and handling of datasets can substantially boost the performance of ML models used in cybersecurity-

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

related applications. The results show that network telemetry offers useful information to evaluate cryptographic readiness without having to access communication content. The proposed framework can analyze traffic characteristics and protocol information, as well as encryption-related features, to determine if the traffic is a legacy cryptographic flow and help organizations prioritize migration activities. The ability is significant due to the number of systems that are deployed in the enterprise environment which are complex and distributed, making it difficult and time consuming to manually locate the cryptographic dependencies.

In addition, this work is important in the field of research because of the combination of network telemetry analysis with the migration strategy for PQC. So far, the focus of PQC research has been on creating quantum-resistant algorithms and assessing their mathematical security properties (Bernstein & Lange, 2017). But it's not the organizations alone that need to be aware of their existing crypto landscapes and identify their migration needs.

Credit authorship contribution statement

Md Shehab Hossain: Writing – original draft, Formal analysis, Conceptualization. Saddam Nasir Chowdhury: Writing – original draft, Formal analysis. Rakesh Kumar Reddy Aduri: Writing – review & editing, Formal analysis, Data curation.

Funding

No external funding was received for this research.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request

REFERENCES

1. Hegde, P. "AI-Powered 5G Networks: Enhancing Speed, Efficiency, and Connectivity." *International Journal of Research Science and Management* 6.3 (2019): 50-61.
2. Ogungbemi, A. T., Adun, H., Adedeji, M., Kavaz, D., & Dagbasi, M. "Does particle size in nanofluid synthesis affect their performance as heat transfer fluid in flat plate collectors?—An energy and exergy analysis." *Sustainability* 14.16 (2022): 10429.
3. Dalal, A. "Cybersecurity and artificial intelligence: How ai is being used in cybersecurity to improve detection and response to cyber threats." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 9.3 (2018): 10-61841.
4. Tiwari, A. "AI-driven content systems: Innovation and early adoption." *Propel Journal of Academic Research* 2.1 (2022): 61-79.
5. Adedeji, M., Abid, M., Adun, H., Ogungbemi, A. T., Alao, D., & Zaini, J. H. "Thermodynamic modeling and exergoenvironmental analysis of a methane gas-powered combined heat and power system." *Applied Sciences* 12.19 (2022): 10188.
6. Hegde, P., & Varughese, R. J. "AI-driven data analytics: Insights for telecom growth strategies." *International Journal of Research Science and Management* 7.7 (2020): 52-68.
7. Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., & Alperin-Sheriff, J. "Status report on the second round of the NIST post-quantum cryptography standardization process." (2020).
8. Dalal, A., & Abdul, S. "AI Powered Threat Hunting in SAP and ERP Environments: Proactive Approaches to Cyber Defense." *Available at SSRN 5198746* (2019).
9. Adun, H., Ishaku, H. P., & Ogungbemi, A. T. "Towards renewable energy targets for the Middle East and North African region: a decarbonization assessment of energy-water nexus." *Journal of Cleaner Production* 374 (2022): 133944.
10. Bernstein, D. J. "Post-quantum cryptography." *Encyclopedia of cryptography, security and privacy*. Cham: Springer Nature Switzerland, 2025. 1846-1847.
11. Tansu, A., Ogungbemi, A. T., & Hocanın, F. T. "The challenges and serviceability of solar power: suggestion on solving the Nigeria energy crisis." *International Journal of Energy Studies* 7.2 (2022): 127-141.
12. Buczak, A. L., & Guven, E. "A survey of data mining and machine learning methods for cyber security intrusion detection." *IEEE Communications surveys & tutorials* 18.2 (2015): 1153-1176.
13. Dalal, A. "Cybersecurity and privacy: Balancing security and individual rights in the digital age." *Available at SSRN 5171893* (2020).

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher

14. Adun, H., Ishaku, H. P., Ayomide Titus, O., & Shefik, A. "3-E feasibility analysis on photovoltaic/thermal application for residential buildings: a case study of Sub-Saharan Africa." *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects* 44.4 (2022): 9901-9919.
15. Dalal, A. "Harnessing the power of SAP applications to optimize enterprise resource planning and business analytics." *Available at SSRN 5422375* (2020).
16. Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., & Smith-Tone, D. "Report on post-quantum cryptography." *Vol. 12. Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology*, (2016).
17. Hegde, P., & Varughese, R. J. "AI-powered network optimization: application of artificial intelligence in optimizing network performance, including self-healing and self-optimizing capabilities." *Int. J. Commun. Netw. Inf. Secur. IJCNIS* (2022).
18. Karmakar, S. "AI-Enhanced SQL Tuning and Execution Plans in Oracle 19c." (2021).
19. Mosca, M. "Cybersecurity in an era with quantum computers: Will we be ready?." *IEEE Security & Privacy* 16.5 (2018): 38-41.
20. Dalal, A. "Revolutionizing Enterprise Data Management Using SAP HANA for Improved Performance and Scalability." *Available at SSRN 5424194* (2018).
21. Polyzotis, N., Roy, S., Whang, S. E., & Zinkevich, M. "Data management challenges in production machine learning." *Proceedings of the 2017 ACM international conference on management of data*. (2017).
22. Preskill, J. "Quantum computing in the NISQ era and beyond." *Quantum* 2 (2018): 79.
23. Hegde, P. "Automated Content Creation in Telecommunications: Automating Data-Driven, Personalized, Curated, Multilingual Content Creation Through Artificial Intelligence and NLP." *Jurnal Komputer, Informasi dan Teknologi* 1.2 (2021): 20-20.
24. Dalal, A. "Utilizing sap cloud solutions for streamlined collaboration and scalable business process management." *International Journal of Current Engineering and Scientific Research (IJCESR)* 6 (2019).
25. Hegde, P., & Varughese, R. J. "Predictive Maintenance in Telecom: Artificial Intelligence for predicting and preventing network failures, reducing downtime and maintenance costs, and maximizing efficiency." *Journal of Mechanical, Civil and Industrial Engineering* 3.3 (2022): 102-118.
26. Shor, P. W. "Algorithms for quantum computation: discrete logarithms and factoring." *Proceedings 35th annual symposium on foundations of computer science*. Ieee, (1994).
27. Sommer, R., & Paxson, V. "Outside the closed world: On using machine learning for network intrusion detection." *2010 IEEE symposium on security and privacy*. IEEE, (2010).
28. Euijong Whang, S., Roh, Y., Song, H., & Lee, J. G. "Data Collection and Quality Challenges in Deep Learning: A Data-Centric AI Perspective." *arXiv e-prints* (2021): arXiv-2112.

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Ekambaram, V. G., Pittala, S. K. & Ashok, V. K. C. "Data-Centric AI in the NISQ Era: Mining Network Telemetry for Quantum-Resistant Cyber Defenses." *Sarcouncil Journal of Applied Sciences* 2.12 (2022): pp 1-10.

Copyright © 2022 The Author(s): This work is licensed under a Creative Commons Attribution- NonCommercial-NoDerivatives 4.0 (CC BY-NC-ND 4.0) International License

Publisher: SARC Publisher