TECH OFFER

Resilient Data Encryption Against Quantum Cybersecurity Attacks

KEY INFORMATION

TECHNOLOGY CATEGORY:
Infocomm - Security & Privacy

TECHNOLOGY READINESS LEVEL (TRL): TRL7
COUNTRY: SINGAPORE
ID NUMBER: TO175341

OVERVIEW

The Internet has become the de-facto medium for many enterprises to carry out their business functions. By relying on public-key encryption to ensure confidentiality and authenticity of data, employees and customers are able to use a variety of public channels via web browsers, emails and mobile apps to send and receive sensitive information securely. However, this promise of confidentiality and authenticity is being compromised with the advent of quantum computers. With the potential rise of exponentially powerful quantum computing, current data encryption algorithms are not resilient enough for such hidden quantum cyberattacks, specifically harvest-now decrypt-later (HNDL) attacks, resulting in data leaks and undermining privacy.

The technology owner has leveraged on their proprietary post-quantum cryptography (PQC) implementation to develop a software module to provide and enhance existing end-to-end data encryption, ensuring resilience to quantum cyberattacks while maintaining confidentiality and authenticity of data. By utilising Key Encapsulation Mechanism (KEM) and JavaScript, it is compliant with evolving cybersecurity standards while being lightweight and dynamic enough to be loaded and executed without installation or configuration. This enables the technology solution to be flexible, scalable and user-friendly.

The technology owner is currently working with an organisation to further develop industrial applicable solutions. The technology owner is seeking collaboration partners, such as system integrators, independent software vendors, solution providers and end-users, who require an enhanced and compliant data encryption for the finance, government and healthcare industries.

TECHNOLOGY FEATURES & SPECIFICATIONS

The technology solution, in a form of a software module, leverages on their proprietary PQC cryptographic implementation to secure confidentiality and authenticity of data. Some specifications of the module include:

- Compliance to National Institute of Standards and Technology (NIST) PQC encryption method
- Utilises combination of ML-KEM-768 (FIPS 203) and AES FIPS 197 algorithms for secure key establishment
- Client-side JavaScript library with possible enterprise integration with hardware security modules (KSM), e.g. OTP device
- No installation or configuration required
- Optimised to run dynamically on devices and platforms

With the above specifications, this quantum-resistant software solution has the following features:

- Supports and enhances existing end-to-end data encryption to be quantum resilient
- User friendly with processes being executed at backend.
- Does not require technical expertise to deploy, use and maintain
- Flexibility in integration to new or existing infrastructures
- Lightweight and scalable for fast and rapid deployment

POTENTIAL APPLICATIONS

With the potential rise of quantum cyberattacks, especially HNDL attacks, private information and data can potentially be vulnerable and compromised. Hence, any application transmitting sensitive data via web browser or mobile applications requiring heightened cybersecurity will greatly benefit from it. Examples of such applications include, but not limited to:

- Digital interaction and conversations with customers
- Customer portal for transaction and filing purposes
- Secure file transfer and email to via internet or intranet
- Digital entry requiring sensitive information
- Online transaction requiring private information

UNIQUE VALUE PROPOSITION

The software module protects against quantum threats, such as HNDL attacks, by leveraging on their proprietary PQC encryption implementation, ensuring secure end-to-end encryption of data between web browser and organisation. Utilising a hybrid combination of ML-KEM-768 and AES FIPS 197 algorithms, it provides compliance to NIST standards to be quantum resilient. With the solution deployed on JavaScript, it is dynamic and integrates seamlessly with existing infrastructure backend, maintaining existing end-user experience. The software is efficient and resource light while being scalable. With the adoption of such technology solution, it enables organisation to pre-emptively fortify their digital security for an incoming post-quantum world.