ICMetrics based Industrial Internet of Things (IIoT) Security in the Post Quantum World

Ruhma Tahir, *Member, IAENG* and Klaus McDonald-Maier

***Abstract*— We are moving into an era of autonomous Industrial Internet of Things world; its security must be considered a crucial element. To maintain the current growth rate in Industrial Internet of Things, future threats related to quantum computing era need utmost attention. This research, in its preliminary stages is a major step in this direction and aims to design an ICMetrics based Industrial Internet of Things security framework for the post quantum era.**

***Index Terms*— ICMetrics, Industrial Internet of Things (IIoT), Lattice based cryptography**

I. Introduction

Industrial Internet of Things (IIoT) is emerging powerfully in industrial processes. The industrial internet of things (IIoT) is directed at a multitude of industries such as manufacturing equipment monitoring, smart warehousing, building automation, automotive industry, aerospace and so much more. IIoT holds great potential for improved communications, productivity, quality control, supply chain efficiencies and general business operations.

Quantum computing is the paradigm shift that is taking place to handle the potentially enormous amounts of digital IIoT data associated with the above application areas. This shift dramatically increases the calculation and computational capacity for these huge amounts of digital data at hand. However, the use of IIoT in the quantum era creates new vulnerabilities and potential avenues of attacks. To successfully implement an IIoT ecosystem, it is very crucial to improve everything pertaining to security of commutations in IIoT. So, whether its connecting cars, outfitting smart buildings, bringing intelligent cities online or manufacturing in factories of the future, the security should be implemented by design into the IIoT ecosystem to deal with the threats associated with quantum computing. If the security is built into the IIoT systems by design at an early stage of the product lifecycle, the incorporation of security is much easier and more cost effective.

The security of the IIoT applications can be implemented by design utilising the ICMetric technology. The ICMetric technology [1-2] uses hardware/ software features and the specification of a device in the IIoT setting to associate an identity with the IIoT entity. The ICMetric of the device is based on features determined at run time, thereby effectively safeguarding against issues related to device identity theft. Further security principles can be layered built on top of the ICMetric of the IIoT device.

To design a cryptosystem for the IIoT that is safe from the threats of quantum computing, we propose the use of the obtained ICMetric in combination with a Lattice based cryptosystem – NTRUencrypt, utilising an ICMetric based NTRU framework for IIoT applications we referred to as Q-ICMetrics. Lattices have emerged as a very attractive foundation for cryptography due to their worst-case hardness and that they are secure even against quantum computers. Through the combination of these major schemes we look to design/ develop a solution that will deliver security services like key generation, authentication, non-repudiation and confidentiality based for the IIoT in the post quantum era.

II. Design goals

IIoT security for the post quantum era is a huge challenge and indifferent from traditional software based security solutions for IoT systems. It's a completely new security landscape these has its own goals. IIoT systems have a long product deployment and usage lifetime and rarely have someone involved in managing them. The top priorities for IIOT systems are productivity, reliability, efficiency and safety. IIoT systems need to be up and running for years, with rare opportunities for downtime. Specifically, Industrial control systems often can't be updated during the lifetime of the product. Therefore, there is need for a robust security design that can meet the demands of IIoT applications keeping in mind the challenges of the post quantum era at the same time.

III. Q-ICmetrics

In this research, we aim to improve the security and performance properties without significantly increasing the IIoT device's energy consumption. We propose an ICMetrics based cryptosystem using NTRUEncrypt that aims to safeguard against possible threats posed by quantum computing. The proposed system formally referred to as Q-ICMetrics will perform authentication, confidentiality, integrity and non-repudiation of data exchanged between devices part of the IIoT application. Due to the resource restrictions imposed on embedded systems, our major objective in designing the new security model is to minimize cost-effect of communication overhead and computation overhead while maintaining required levels of security in the post quantum era.

R. T. is with the Computer Science and Electronic Engineering Department, University of Essex, Colchester, CO2 3SQ (phone: 44-1473-767856; e-mail: rtahir@ essex.ac.uk).

K. M. is with the Computer Science and Electronic Engineering Department, University of Essex, Colchester, CO2 3SQ (e-mail: kdm@essex.ac.uk).

A. ICMETRICS

IIoT applications rely on using stored secret keys for security. Stored keys in IIoT applications can lead to key theft by infiltration or simple theft. When the secret keys of a system are exposed, the security of the system is compromised in its entirety. Using characteristic features specific to a device, an identification can be generated for every IIoT device. The proposed system is based on an emerging security technology called Integrated Circuit Metric (ICMetric) that extracts the inherent features of a device to generate a unique device identification [1-2]. The device identification formally called the ICMetric is generated each time it is required and discarded thereafter thus entirely eliminating key theft from the IIoT device. The ICMetric technology uses variable internal features for identifying a device part of the IIoT. This is the opposite of the conventional hardware fingerprinting techniques that use static features that are easy to capture, thereby rendering the hardware fingerprint useless.

The generation of the ICMetric is a two-phase process, *i.e.* calibration phase and the operation phase. The calibration phase is applied once when the ICMetric is required for the device part of the IIoT. In this phase feature values are extracted from the device and normalized. The obtained feature maps of the device are studied for their standard deviation, confidence interval, interquartile range and skewness. A multitude of feature values are read to ensure a wide coverage of features. In the operation phase the feature values are combined to form an ICMetric. Two techniques can be used for combining the individual feature values, *i.e.* feature addition and feature concatenation.

B. NTRUEncrypt

NTRU is a post quantum lattice based cryptosystem that supports encryption and decryption. We propose the use of NTRU for providing ICMetric based post-quantum security services for IIoT devices. NTRU is a public key cryptosystem proved to be secure against quantum computing attacks. It is also researched to be memory and energy efficient [3-5].

IV. ANALYSIS OF Q-ICMETRICS

In this research, the ICMetric technology is utilized to generate keys based on the hardware/software characteristics and specification of the device part of the IIoT, thereby enabling device identification/ verification. This provides an effective means to address the issues related to storage of key, thereby safeguarding against the major threat of key compromise.

All the associated benefits of IIoT are dependent on sending and receiving accurate data and commands to the correct device in the IIoT application. This can be achieved by using the ICMetric technology, where all IIoT devices have a unique ICMetric, which they use for identification throughout their long lifecycle. Knowing where your data is being sent and which device its coming from in an absolute essential in IIoT. So, may it be authenticating the IIoT devices, encryption to enable secure communications or data integrity to ensure that the messages are not altered in transit. A IIoT device encountering a problem in the can be identified remotely based on its ICMetric. Non-repudiation is an inferred security goal of the design, since generating the ICMetric from a range of features that are unique to a computation device prevents an entity from denying a particular action performed by their IIoT device.

An advantage of the scheme presented here, is that human intervention is not required at any point during the lifecycle of its secure functioning. This is particularly important from the IIoT perspective, since this will ensure its usefulness while securely transmitting data between the IIoT devices. Thus, the security functions of our post quantum framework are based on ICMetric data derived from the respective devices and integrate with the NTRU. NTRU is the post quantum cryptosystem proposed in our research for providing IIoT security based on the ICMetric of each device. NTRU is very well suited for IIoT applications due to its computational efficiency and low memory requirement.

V. CONCLUSION AND FUTURE WORK

The Industrial Internet of Things is improving operational efficiencies for global industrial systems at a pace never seen before. This consequentially brings a pressing need for major changes to the security landscape for the IIoT to deal with the threats of quantum computing. In this work, we propose employing NTRU coupled with the ICMetric technology, to provide security in the IIoT.

Our future plan is to evaluate the research here through experiments and analysis. We are confident that our proposed architecture will be an efficient and viable solution for providing comprehensive post quantum security in IIoT.

REFERENCES

[1] Papoutsis, E., "Investigation of The Potential of Generating Encryption Keys for ICMetrics.", PhD Thesis, The University of Kent, Canterbury, June 2009*).*

[2] Tahir, H.; Tahir, R.; McDonald-Maier, K. "Securing MEMS Based Sensor Nodes in the Internet of Things." In Proceedings of the Sixth International Conference on Emerging Security Technologies, Braunschweig, Germany, 3–15 September 2015.

[3] O. Collen Marie, "Efficient NTRU implementation," Master's thesis, Worcester Polytechnic Institute, 2002.

[4] M. Monteverde, "NTRU Software Implementation for Constrained Devices," Master's thesis, Katholieke Universiteit Leuven, 2008.

[5] A. Boorghany, S. B. Sarmadi, and R. Jalili, "On Constrained Implementation of Lattice-Based Cryptographic Primitives and Schemes on Smart Cards," *ACM Trans. Embed. Comput. Syst.*, vol. 14, no. 3, pp. 42:1–42:25, Apr. 2015.