نموذج تحليلي للأمن السيبراني مبني على أساس تشفير خفيف الوزن لإنترنت الأشياء

عمر أحمد محمد عبد القادر

رسالة مقدمة لاستكمال متطلبات درجة الدكتوراه في العلوم (علوم الحاسبات)

تحت إشراف
الدكتور: فيجي ثايانانثان
أستاذ دكتور: كمال منصور جمبي

١. المستخلص

أصبحت التقنيات الواعده مثل M2M, IoT, CPS تتطور بشكل متسارع وتاخذ زخم كبير وإهتمام كثيف في كلاً من الأبحاث الأكاديميه والصناعيه. توفر البنيه التحتيه للشبكات الخلويه والشبكات المخصصه والتطور الحاصل موخراً في شبكات الاتصالات الخلويه LTE شجعت الباحثين من إستغلال هذه الشبكات الخلويه من أجل بناء شبكة إتصال بين الآلآت حتى تتمكن من تبادل البيانات فيما بينها بدون تدخل الإنسان أو من خلال تدخل بسيط. ومن الواضح أن الإتصال المباشر بين الآلآت يكون أكثر عرضه للهجمات الاليكترونيه والمعلوماتيه. عليه فإن المواضيع ذات الصله بالأمن السيبراني والمعلوماتي لاتزال هاجس يقلق الباحثين, ولابد من إيجاد حلول تضمن سريه وخصوصيه هذه البيانات لتحصل هذه التقنيات الواعده على قبول وثقة المستخدمين.

تعتبر هذه الآلآت الآت فائقة الصغر وذات قدرات محدوده من حيث القدره علي إجراء علميات حسابيه سريعه وتستهلك قدر عالي من الطاقة وليس لديها ذاكرة تخزين عاليه أو معالج قوي لأداء العمليات المختلفه.

طرق التشفير التقليديه المقترحه تتطلب قدره عاليه وفائقه من السرعه في إنجاز العمليات الحسابيه وتستهلك طاقة عاليه من الآلآت وتتطلب أيضاُ ذاكرة تخزين عاليه ومعالج قوي لتتمكن من أداء العمليات المخلتفه بسرعه فائقة. عليه فإنه ليس بالإمكان تبني طرق التشفير التقليديه من أجل توفير السريه والخصوصيه للبيانات الناتجه من الآلآت أو في نقل هذه البيانات من خلال الشبكات المخلتفه. من خلال ماسبق ذكره, يتضح لنا جلياً أنه لابد من عمل تعديلات أو تحسينات على طرق التشفير التقليديه المتسخدمه حالياً من أجل تقديم مقترح بروتوكولات وطرق تشفير خفيفة الوزن تتلائم مع إمكانيات وقدرات

الآلآت الفائقة الصغر.

تهدف هذه الاطروحه الى تقديم مقترح طرق تشفير تمتاز بأنها منصه مستقله وخفيفة الوزن توفر حلول لمشاكل السريه والخصوصيه في بيئة IoT و M2M .

ويتكون المقترح البحثي من مرحلة التسجيل ومرحلة توليد مفاتيح السر ومرحلة تبادل مفاتيح السر ومرحلة توصيل البيانات المشفره بطرق آمنه. وقد تم تبني فكرة البلوك شين للأمن السيبراني من أجل توفير حماية للبيانات الناتجه من قبل أجهزة انترنت الاشياء وكذلك إضافة خاصية الشبكات الموزعة على المقترح البحثي.

وقد أثبتت نتائج تحاليل التجارب أن المقترح البحثي يوفر حماية للأمن السيبراني والمعلومات الصادرة من أجهزة إنترت الأشياء وأنه مقاوم ضد الهجمات السلبيه (التي تستهدف الحصول على البيانات دون إلحاق أضرار) والإيجابيه (التي تستهدف الحصول على البيانات وكذلك إلحاق أضرار جسيمه). وكذلك أن المقترح البحثي يحقق الأهداف الرئيسيه المرجوه منه وهي أن يكون خفيف الوزن في أجراء العمليات الحسابيه ولايستنفذ طاقة عاليه من الآلآت.

Analytical Cybersecurity model based on lightweight Cryptography for IoT

By

Omer Ahmed Mohamed Abdulkader

A thesis submitted to King Abdulaziz University in fulfillment of the requirements for the degree of Doctoral of Science in Computer Science

Supervised by

Associate Professor: Vijey Thayananthan

Professor: Kamal Mansor Jambi

2. ABSTRACT

The new promising technologies Internet of Things (IoT), Machine-to-machine (M2M), Cyber-Physical System (CPS), and Blockchain (BC) are rapidly evolving and gaining intensive interesting in both academic and industrial research. The existences cellular, ad-hoc networks infrastructure and recent advances such as long-term evolution (LTE) technology encourage researchers to exploit them to build coexist communication between devices. Obviously, machine type communication (MTC) is more vulnerable to cyber risks and threats. Therefore, cyber security issues remain obsession worries to researchers and need to be addressed to gain public acceptance and trust. Tiny devices are also vulnerable to all types of cyber threats created from neighbouring resources. M2M resources constrained in term of computational, energy, processing and storage capabilities. Despite the evolving threats with these constraints, a conventional cryptosystem is suffering from computational overhead and energy consumption. Therefore, existing security solutions and approaches cannot adopt for tiny devices which face the evolving cyber threats or attacks. Based on aforementioned, an optimization on existing cryptosystem which deals with a lightweight cryptographic protocol considered as urgent needed.

This thesis aims to propose an independent platform which is an analytical solution based on lightweight cryptography for IoT and M2M devices. The proposed platform consists of the registration phase, key generation phase, key exchange, and message delivery in a secure manner. Blockchain based cybersecurity has been implemented to provide more security for the proposed model to protect IoT devices generated data and to provide distributed nature for the proposed model. The experimental analysis shows that the proposed platform is providing cyber

protection and resist against passive and active attacks. Also, it achieves low computational overhead and low energy consumption.

Keyword:

Cyber security, lightweight cryptographic, analytical security model, privacy, Blockchain, computation and energy consumption