آلية برمجية لحماية انترنت الأشياء في البنية الموزعة

بروتوكول نقل القياس عن بُعد في قائمة انتظار الرسائل (إم كيو تي تي) هو بروتوكول مراسلة واعد يُستخدم في إنترنت الأشياء. ولكن، مع النمو السريع للأجهزة المتصلة بالإنترنت والكم الهائل من البيانات التي يمكن إنشاؤها وتبادلها في بيئة إنترنت الأشياء، يمكن أن تواجه إم كيو تي تي العديد من التحديات ، مثل أعباء الأداء المرتفعة، وازدحام الشبكة، ومشكلة قابلية التوسع ، وتعقيد ادارة الأمان. هذا لأن بنية إم كيو تي تي الحالية تعتمد على وسيط مركزي في السحابة مسؤول عن تسليم البيانات بين العملاء (من الناشر إلى المشترك) وتنفذ آلية مصادقة ثقيلة تعتمد على بروتوكول التشفير، طبقة مآخذ التوصيل الآمنة / طبقة النقل الآمنة (إس إس إل/تي إل إس). في هذه الحالة ، لن تتمكن بنية إم كيو تي تي القائمة على السحابة من تلبية متطلبات إنترنت الأشياء، وخاصة تطبيقات إنترنت الأشياء المعقدة التي تحتاج إلى استجابات سريعة ومعالجة في الوقت الفعلي وأتمتة عالية المستوى ، كما هو الحال في إنترنت الأشياء الصناعي (آي آي أو تي).

نتيجة لذلك ، تقترح هذه الأطروحة بنية إم كيو تي تي قائمة على الضباب حيث يتم توزيع الوسطاء في طبقة الضباب والتواصل مع بعضهم البعض باستخدام آلية التجسير الديناميكي للسماح بتسليم البيانات من الناشر إلى المشترك من خلال أكثر من وسيط واحد. بالإضافة إلى ذلك ، تقدم الأطروحة مخطط مصادقة متبادلة خفيف الوزن يعتمد على وظيفة التجزئة وعملية إكس اور. يتم نشر مدير المصادقة في كل وسيط لإنشاء معلمات المصادقة وإجراء المصادقة لكل مجموعة من العملاء / الوسطاء المتصلين بهذا الوسيط لتحقيق إدارة أمان مستقلة. تم تحليل أمان النظام باستخدام التحليل الرسمي وغير الرسمي باستخدام أداة التحقق الآلي لبروتوكولات وتطبيقات أمان الإنترنت (أفيسبا). وأظهرت النتائج أن المخطط آمن ويمكنه مقاومة الهجمات الشائعة مثل انتحال الهوية وإعادة التشغيل وهجمات التنصت. علاوة على ذلك ، تم تقييم أداء المخطط ومقارنته مع المخططات الأخرى ، وأظهرت النتائج أن المخطط تفوق في الأداء وكان أكثر كفاءة.

اسم الطالب: حسن كردي

اسم المشرف: د. فيجي ثايانانثان

SOFTWARE MECHANISM FOR SECURING INTERNET OF THINGS IN DISTRIBUTED ARCHITECTURE

Message Queue Telemetry Transport (MQTT) protocol is a promising messaging protocol used in IoT. However, with the rapid growth of internet-connected devices and the tremendous amount of data that could be generated and exchanged in an IoT environment, MQTT can encounter many challenges, such as increasing performance overhead, network congestion, scalability issue, and complexity of security management. This is because the current MQTT architecture relies on a central broker in the cloud responsible for delivering data between clients (from the publisher to the subscriber) and implements a heavyweight authentication mechanism based on the cryptographic protocol, Secure Sockets Layer/Transport Layer Security (SSL/TLS). In this case, cloud-based MQTT architecture will be unable to meet IoT requirements, especially the complex IoT applications that need fast responses, real-time processing, and high-level automation, such as in the Industrial Internet of Things (IIoT).

As a result, this thesis proposes a fog-based MQTT architecture where brokers are distributed in a fog layer and communicate with each other using the dynamic bridging mechanism to allow delivering data from the publisher to the subscriber through more than one broker. In addition, the thesis presents a lightweight mutual authentication scheme based on the hash function and XOR operation. An authentication manager is deployed in each broker to generate authentication parameters and conduct authentication for each group of clients/brokers connected to that broker to achieve independent security management. The scheme's security was analyzed using informal and formal analysis using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The results showed that the scheme is safe and can resist common attacks such as impersonation, replay, and eavesdropping attacks. Furthermore, the scheme's performance was evaluated and showed that it outperformed and it was more efficient compared with other schemes.

Student Name: Hassan Kurdi

Supervisor: Dr. Vijey Thayananthan