حماية الخصوصية في انترنت الأشياء المعتمدة على الحوسبة الضبابية

الطالب : عدنان أحمد أبي سن

اشراف : أ. د. فتحي البرعي عيسى

حماية الخصوصية واحدة من أكثر التحديات التي تواجه مستقبل انترنت الأشياء و الذي يعد بتوفير خدمات أكثر ذكاءً و تطوراً في حياتنا. هذا البحث يعالج هذه المشكلة من خلال عرض ثلاثة منهجيات جديدة (المبادلة, المضاعفة, الأعمى) اعتماداً على الحوسبة الضبابية حيث لكل نهج مجموعة من التقنيات المختلفة و التي يقدم كل منها حلاً للمشاكل المفتوحة الموجودة في تقنيات حماية الخصوصية الحالية. أيضاً يمهد هذا البحث الطريق أمام أفكار و طرق جديدة من خلال توظيف خصائص الحوسبة الضبابية لتحسين مستوى الخصوصية و الأداء معاً بالإضافة لدعم أنواع جديدة من تطبيقات انترنت الأشياء كتلك الحساسة للتأخير. تتكامل جميع الطرق المقترحة في منصة واحدة ديناميكية يمكن استخدامها في أي نظام ضمن انترنت الأشياء. خلال البحث تم تقديم دراسة مرجعية حول منهجيات حماية الخصوصية المختلفة مع تصنيف مقترح اعتماداً على درجة الثقة اللازمة بالإضافة إلى دراسة مرجعية حول الحوسبة الضبابية و مقارنتها بالسحابية.

من خلال التحقيق و المحاكاة أكدت النهج المقترحة في هذا البحث تفوقها على النهج الأخرى الموجودة وفقاً لمعامل مستوى الخصوصية و مستوى الأداء. لذلك نؤمن أن النموذج المقترح يمكن تطبيقه ضمن معظم تطبيقات انترنت الأشياء الحقيقية كالمدن الذكية, البيوت الذكية, إدارة الحشود, الحساسات تحت الماء, التطبيقات العسكرية, التطبيقات الطبية, و التطبيقات المعتمدة على خدمة المواقع و غيرها. أخيراً تحديات جديدة و أفكار جديدة تم اقتراحها للعمل عليها مستقبلاً في بيئة انترنت الأشياء.

Preserving Privacy of Fog Computing-Based Internet of Things

Student: Adnan Ahmed Abi Sen

Supervised By : PROF. Dr. Fathy Albouraey Eassa

ABSTRACT

Privacy is one of the greatest challenges for the future of Internet of Things (IOT), which has promised to provide smarter and more sophisticated services in our life. This research addressed this problem by presenting three approaches (SWAPPING, DOUBLE, and BLIND based on FOG) with different techniques, and providing solutions for most of the limitations and open problems of previous approaches. This research has paved the way to novel methods for protection privacy by employing Fog computing and its properties to enhance both the privacy and the performance level, in addition to supporting new types of applications like the sensitive to latency. An integrated dynamic model was introduced for collecting all proposed methods in one framework, which can be used in any IOT system. A survey of privacy approaches of the IOT with new classification, and to survey of Fog computing were done, in addition to comprehence comparison between Privacy vs. Security, Cloud vs. Fog. Implementation and simulation, proposed approaches, confirmed their superiority to others, according to privacy and performance factors. We believe that our model can be applied to most of real environments in IoT such as Smart City, Smart Home, Crowd Management, Smart Health, Smart Business, Location Based Services, WSNs and RFIDs applications, Underwater Sensor Networks, etc., and that will contribute to developing and enhancing the future of services. Finally, new challenges, ideas, and applications were suggested for future works in the IOT domain