الأمان الثلاثي للمطابقة المشفرة لبيانات بصمات الأصابع في السحابة

بيان طه الزهراني

بحث مقدم لنيل درجة الماجستير في العلوم
(تقنية المعلومات)

د.فهد السلمي

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
رمضان ١٤٣٩هـ – مايو 2018 م

الأمان الثلاثي للمطابقة المشفرة لبيانات بصمات الأصابع في السحابة

بيان طه الزهراني

المستخلص

في الآونة الأخيرة، تلعب البيانات البيومترية دورًا مهمًا كأداة لتوثيق الهوية. واعتبرت المصادقة الحيوية تكنولوجيا واعدة تستخدم عبر أنظمة متعددة لتوفير التحقق الموثوق به. ومع ذلك، لا يزال تصميم نظام فعال وآمن للمصادقة الحيوية في بيئة الحوسبة السحابية يمثل تحديا بحثيا. لذلك الهدف من هذه الدراسة هو معالجة مسألة الأمن والخصوصية للبيانات الحيوية (أي بصمات الأصابع) المخزنة في السحابة من خلال اقتراح خوارزمية BioStash. تحقق خوارزمية BioStash مستوى عالٍ من الأمان والخصوصية من خلال استخدام ثلاث طبقات للأمان. أولاً، تقوم خوارزمية BioStash بتحويل وتشفير بيانات بصمة المستخدم. ثانياً، تقوم خوارزمية BioStash بتضمين جزء من المفتاح السري المشترك داخل البصمة المشفرة. في الطبقة الأخيرة، تقوم خوارزمية BioStash بتوزيع جميع المشاركات على سحب متعددة في نفس الوقت. في عملية التحقق من البصمة، هذه الدراسة تطابق بصمات الأصابع في شكلها المشفر دون الحاجة الى فك التشفير عن البيانات من أجل الحفاظ على الخصوصية. بالإضافة إلى ذلك، يستخدم BioStash تقنية تعدد المهام لمعالجة المشاركات المتعددة عبر عدة غيوم بالتوازي. تظهر النتائج التجريبية أن نظام BioStash يحقق وقت مطابقة أسرع ودقة مقاربة مقارنة مع خطوط الأساس. علاوة على ذلك، أثبتنا أن نظامنا المقترح يوفر حلاً واعدًا لتحسين أمان وخصوصية بيانات بصمات الأصابع في السحابة.

BioStash: Triple Security for Encoded Matching of Fingerprint Data in the Cloud

Bayan Taha Alzahrani

A thesis submitted for the requirements of the degree of Master of Science in Information Technology

Supervised By
Dr. Fahad Alsolami

Faculty of Computing and Information Technology
KING ABDULAZIZ UNIVERSITY
JEDDAH-SAUDI ARABIA
RAMDAN 1439 H – May 2018 G

BioStash: Triple Security for Encoded Matching of Fingerprint Data in the Cloud

Bayan Taha Alzahrani

ABSTRACT

Recently, biometric data plays an important role as an identity authentication technique. Biometric authentication considered a promising technology used across multiple systems to provide a reliable verification. However, designing a biometrics authentication system that are effectively secure in the cloud environment remains a research challenge. In this research, we aim to handle privacy and security issue of biometrics data (i.e. fingerprints) in the cloud by proposing BioStash algorithm. BioStash algorithm achieves high-level of security and privacy by applying triple security layers. First, BioStash algorithm transforms and encrypts user's fingerprint data. Then, BioStash embeds a shared secret key inside the encrypted fingerprint. At the final layer, BioStash algorithm distributes all the shares over multiple clouds. During fingerprint matching process, BioStash matches the fingerprints in their secure encoded form without decoding the data in order to preserve the privacy. In addition, BioStash uses multithreading to handle multi-shares over multiple clouds in parallel. The experimental results show that BioStash system has a faster matching time while achieves comparable accuracy compared to the baselines. Further, we proved that our proposed system provides a promising solution to improve privacy and security of fingerprint data in the cloud.