Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Computer Science

Preserving Security of Data On The Cloud Using Deep Learning

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
Is a Partial Fulfillment of The Requirements
for the Degree of Master of Science
in
Computer Science**

By

Mohammed Fawzi sheet Alqataan

Supervised by

Asst. Prof.

Milad Jader Saeed

2023 A.D. **1444 A.H.**

Abstract

Cloud computing has now become widespread in different fields, including medical, scientific, and business. Each type meets different needs and according to the purpose designed for it. The most important purpose in the selection process is the security of the data that will be used in the cloud.

Deep learning is one of the most important techniques based on artificial intelligence. It has become widespread at present, because of its high efficiency and flexibility, which conform according to training data rules. This technology has been used to preserve the security of the data inside the cloud. Through this technology, you will get a highly secured and unapproachable cloud, only by real permission.

This thesis provides solutions to the problems of authentication, which often causes problems for the cloud user if it falls into the hands of the wrong person where it is possible to exploit the account for the wrong purposes.

For this purpose, a private cloud was designed, and authentication was done through deep learning using Python 3.10 language. Deep learning algorithms were applied to a real cloud. It was designed and made to have the same characteristics, as any currently used cloud, but with security additions. Important and serious steps have been taken to ensure that the person who owns an account within this cloud is the same authorized person, and no one else can use it. The client's account will remain secured and not subject to impersonation through deep learning algorithms. To log in to the cloud, two techniques are used. The first one is face detection for each image captured for use and the second one is recognition of the liveliness of the image sent for matching to detect if it is a live image or not. If this condition is achieved, only the account owner can open and use the cloud. In this thesis, we opened a way to verify the identity of the user. Moreover, action is taken against any person who tries to use an account that does not belong to him by blocking and taking pictures of the attacker.

To conclude, we obtained a very strong authentication through the use of the proposed system. In this way, whoever tries to log in must have the username, password and face matching. This results in achieving a very high speed which in turn does not constitute a burden on the customer. On average the time spent does not exceed more than two seconds. The threshold of the liveliness of the image was 0.3. If it was less than this, it is not considered to be life. The threshold of face difference was 0.49 to give an allowable amount that might be recorded in case of a slight change or low light.

وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم علوم الحاسوب

الحفاظ على امن البيانات على السحابة باستخدام التعلم العميق

رسالة مقدمة

الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل

كجزء من متطلبات نيل شهادة ماجستير علوم في

علوم الحاسوب

من قبل

محمد فوزي شيت القطان

بإشراف

أ.م ميلاد جادر سعيد

١٤٤٤ هـ ٢٠٢٣ م

خلاصة

أصبحت الحوسبة السحابية الآن منتشرة على نطاق واسع في مختلف المجالات، بما في ذلك الطبية والعلمية والتجارية. حيث ان كل نوع يلبي احتياجات مختلفة ووفقًا للغرض المصمم له. من أهم اسباب اختيار نوع محدد من أنواع السحابة هو أمانُ البيانات التي سيتم استخدامُها في السحابة.

التعلُم العميق من أهم التقنيات المعتمدة على الذكاء الاصطناعي، وقد انتشر في الوقت الحاضر لما يتمتع به من كفاءة ومرونة عالية يكتسبها من قواعد بيانات التدريب. تم توظيف هذه التقنية للحفاظ على أمان البيانات داخل السحابة. حيث سيتم الحصول على سحابة آمنة للغاية ولا يمكن الوصول إليها ، إلا بإذن حقيقي.

تقدم هذه الرسالة حلولاً لمشاكل الوثوقية التي غالباً ما تسبب مشاكل لمستخدم السحابة إذا وقعت في أيدي الشخص الخطأ حيث يمكن استغلال الحساب لأغراض سيئة ومضرة. ولهذا الغرض ، تم تصميم سحابة خاصة ، وتمت المصادقة من خلال التعلم العميق باستخدام لغة Python 3.10. كما تم تطبيق خوارزميات التعلم العميق على سحابة حقيقية. تم تصميمها وصنعها لتكون لها نفس الخصائص والأدوات ، مثل أي سحابة مستخدمة حاليًا، لكن مع إضافات امان جدية. تم اتخاذ خطوات مهمة للتأكد من أن الشخص الذي يمتلك حسابًا داخل هذه السحابة هو نفس الشخص المصرح له ليدخل ويستخدم حسابه الخاص، ولا يمكن لأي شخص آخر استخدامه. وبهذا سيبقى حساب العميل آمنًا ولن يخضع لانتحال الهوية. لتسجيل الدخول إلى السحابة، يتم استخدام طريقتين. الأول هو اكتشاف الوجه لكل صورة تم التقاطها للاستخدام والثاني هو التعرف على حيوية الصورة المرسلة للمطابقة لاكتشاف ما إذا كانت صورة حية أم لا. إذا تم تحقيق هذا الشرط، يمكن فقط لمالك الحساب فتح السحابة واستخدامها. في هذه الرسالة، قدمنا طريقة للتحقق من هوية المستخدم. علاوة على ذلك، يتم اتخاذ إجراء ضد أي شخص يحاول استخدام حساب لا يخصه من خلال حظر والتقاط صور للمهاجم.

كنتيجة لذلك، حصلنا على مصادقة جيدة جدًا من خلال استخدام النظام المقترح. بهذه الطريقة، حيث يجب أن يكون لدى أي شخص يحاول تسجيل الدخول اسم المستخدم وكلمة المرور ومطابقة الوجه. نتيجة لاستخدامنا النظام المقترح تم تحقيق سرعة عالية جدًا للتحقق والتي بدورها لا تشكل عبئًا على العميل. كمعدل، لا يتجاوز الوقت المستغرق أكثر من ثانيتين. كما كانت العتبة

لأثبات حيوية الصورة ٠.٣، وإذا كانت أقل من ذلك، فلا تعتبر الصورة حية. اما عتبة اختلاف بين الوجه المخزون والوجه الذي يحاول الدخول لنفس الحساب ٠.٤٩ لإعطاء مساحة عمل مسموح بها للاختلاف بين الوجهين والذي يمكن تسجيله في حالة حدوث تغيير طفيف أو إضاءة منخفضة او وضع جلسة مختلف.