جامعــة الموصـــل
كليـــة الهندســـة

نمذجة كشف وتجنب هجوم انتحال الشخصية في بيئة الحوسبة السحابية

هدى باسم حامد الدباغ

رسالة ماجستير علوم
هندسة الحاسوب

بإشراف

د. توركان أحمد خليل

1440 هـ 2019 م

المُستخلص

الحوسبة السحابية(Cloud Computing) خدمة تحط رحالها في أجهزة حاسوبية نائية عن المُستخدم بعكس التطبيقات التقليدية التي تُخزّن في أجهزة المستخدم ذاتها. تعتمد الحوسبة السحابية على الإنترنت بشكل أساسي من أجل نقل البيانات، الوصول اليها والتعامل معها؛ مقابل دفع مادي زهيد لكل عملية وصول إلى السحابة، فضلاً عن تولّى مقدموا الحوسبة السحابية توفير البرامج، التراخيص، التحديثات، مساحات التخزين، والبنى التحتية نزولاً عند طلب الزبون. على الرغم من محاسن الحوسبة السحابية، إلا إنها سترث عيوب الإنترنت نفسها، ومنها كونها بيئة مُشتركة بين المُستخدمين، وصعوبة تأمين إنترنت مستمر بدون إنقطاع، و تحديد مستوى الخدمة(Service Level Agreement–SLA) المقبولة، فضلاً عن الثغرات الأمنية، والهجمات التي تطرأ على بروتوكول الإنترنتIPv4.

عالجت هذه الدراسة أبرز تلك الهجمات وأخطرها على السحابة الا وهو هجوم إنتحال الشخصية(Spoofing Attack)؛ والذي ينطلق من الحصول على عنوان العميلIP المُسجّل لدى السحابة وإستغلال جميع صلاحياته من أجل مهاجمته بصورة مباشرة، أو مهاجمة السحابة وإستهداف بيانات العملاء وبالتالي إسقاط سمعة المجهّزين السحابيين. وتسليط الضوء على هجوم إنكار الخدمة(Denial of Service–DoS)، أو إنكار الخدمة الموزعة (Distributed DoS)(هذان الهجومان غالباً ما يكونان مبطنان لهجوم انتحال الشخصية)؛ إذ يتم إرسال فيضاً من الحزم المزيفة العنوان الى الوجهة.

ولمعالجة ما يتم تنفيذه من هجمات انتحال الشخصية حاولت هذه الرسالة تكوين أداة للهجوم(Attack Tool) متكاملة وخاصة لسرقة عنوان العميل(الضحية)، ومن ثم انشاء حزم تحمل عنوان الضحية في عقدة المهاجم وارسالها الى الهدف(الوجهة)؛ هذا يعني ان أداة الهجوم تتعامل مع العناوين(IPv4 Auto–assigned Addresses).

وقد أُقتُرحت خوارزمية (Identification Number–Improved Hop Count Filtering–ID_IHCF)، والتي تُعالج الحزم المُستلمة من خلال المرحلتين الآتيتين:

الاولى: يتم فيها تسجيل كل عميل لدى السحابة بإستخدام رقم تعريفي (Identification Number–ID_Cloud)، يُعطَي لكل عميل ويجب أن يُضمّن هذا الرقم مع الحزمة المُرسلة من قبل العميل. في حالة خلو الحزمة من هذا الرقم التعريفي تُهمل الحزمة مباشرة وتُعدّ بأنها حزمة ضارة و المرسل بأنّه مهاجم.

الثانية: تطوير وتحسين خوارزمية كشف ومنع هجوم انتحال الشخصية قائمة على مبدا إستخلاص البعض من الحقول المُضمّنة في رأس بروتوكول الانترنتIP Header، والعنوان الفيزيائي لآخر عقدة موجّهة للحزم(لغرض تحديد المسار)Physical Address، ورقم منفذ البروتوكولTCPأوUDP(بحسب التطبيق المستخدم)؛ وتُخزّن هذه القيم في السحابة في جدول يدعى(Add2HC) من أجل عملية تصفية الحزم(Packet Filtering) قبل وصولها الى الخادم. وسميت بخوارزمية تصفية عدد القفزات المحسّنة (Improved Hop Count Filtering–IHCF).

تمت المحاكاة بإستخدام برنامج المحاكاة للشبكات والانظمة الموزعة "أوبنت" (OPNET Modeler 14.5A) لأغراض تقييم وفحص أداء الشبكة المُقترحة بعد تطبيق الخوارزمية ID_IHCF، وتطبيق أنواع هجمات الإنتحال(هجوم التخفي Hiding، الإنعكاسReflection، وإنتحال الهويةImpersonation Attack) في حالات هجوم DoS،DDoS. فضلاً عن مقارنتها مع الاساليب التقليدية للكشف عن هجوم الأنتحال بإستخدام الجدران النارية وأمن بروتوكول الإنترنتIPsec، وأيضاً برتوكول الإنترنت الإصدار السادسIPv6. أثبتت النتائج قدرة الخوارزمية المُقترحة على كشف هجوم الإنتحال ومنعه، وبأفضل إستجابة ممكنة عند مقارنة النتائج بالسيناريوهات الاخرى.

Abstract

Cloud Computing is a service that sets on remote devices unlike the traditional applications that are stored in the user's own devices. Cloud computing relies primarily on the Internet for transfer, access and handling the data ; for every cloud usage the user pays fees, as well as cloud computing providers providing software, licenses, updates, storage space, and infrastructure at customer demand. Despite the advantages of cloud computing, it will inherit the same disadvantages of the Internet, including a shared environment and resources, the difficulty of guaranteed continuous Internet without interruption, and determine the level of service (Service Level Agreement-SLA), as well as security vulnerabilities, and attacks on IPv4.

This study processes the most prominent and serious attacks on the cloud; that called the Spoofing Attack, which is based on obtaining the IP address of the user’s cloud and exploiting all its powers to directly attack it, attack the cloud, target customer data and thereby discard the reputation of cloud providers. Highlighting Denial of Service-DoS or Distributed DoS (these attacks are often shielded from Spoofing Attacks); fake packets are sent to the destination.

In order to address the spoofing attacks, this study attempted to create an integrated attack tool specifically to steal the victim's address, and then to create packages with the victim's address at the attacker's node and send them to the destination; with IPv4 (Auto-assigned Addresses).

The Identification Number-Improved Hop Count Filtering-ID_IHCF algorithm, which deals with received packets, has been processed through the following two phases:

First: Each customer is registered in the cloud using a Identification Number (ID_Cloud), this ID_Cloud must be included with the packets sent by the customer. If the packet is free from this ID, the

packet is directly ignored and considered to be a malicious packet and the sender is an attacker.

Second, the development and improvement of the detection and prevention algorithm of the spoofing attack based on the principle of extracting some of the fields included in the IP header, the physical address of the last node(to determine the route), and the port number of the TCP or UDP protocol (according to the application used). These values are stored in the cloud in a table called (Add2HC) for Packet Filtering before it reaches the server. It is called the Improved Hop Count Filtering-IHCF.

Simulated using the OPNET Modeler 14.5A simulation software for evaluation and testing of the proposed network performance, after the implementation of the ID_IHCF algorithm and application of types of spoofing attacks (Hiding, Reflection, and Impersonation Attack) in DoS, DDoS attacks; As well as its comparison with traditional methods of detecting spoofing attacks using firewalls, IPsec, and IPv6. The results demonstrated the ability of the proposed algorithm to detect and prevent spoofing, and the best possible response when comparing results with other scenarios.

University of Mosul
College of Engineering

Simulating the Detection and Avoidance of Spoofing Attack in Cloud Computing Environment

Huda Basim Hamid Al-Dabbagh

M.Sc. Thesis
Computer Engineering Department

Supervised by

Dr. Turkan Ahmed Khaleel

2019 A.D. **1440 A.H**