Intrusion Detection System in Cloud Computing Using Coulomb and Franklin Optimization Algorithm with Support Vector Machine

Prepared by

Fatima Issa Khalaf

Supervisor By

Dr.Omar Al tarawneh

Abstract

In light of the development of technology and the spread of electronic services provided by institutions via the Internet to save time and effort, and the emergence of cloud computing (CC) and its adoption by these institutions to save resources and reduce costs, as a result of these services, we have a huge amount of sensitive and important data that cloud providers must provide security and protection from any attack. It may be stolen or tampered with, and for this it is important to use an intrusion detection system (IDS), which in turn analyzes and processes data received from cloud computing in order to find any suspicious activity or behavior and enhance the security of the system. Due to the huge amount of data received from CC networks which needs to be processed in real time. This will lead to a lack of efficiency in the work of IDS as it takes a long time to analyze this amount of data. Therefore, researchers presented many studies

that address methods and strategies to improve the performance of IDS to resolve this problem. In this thesis, the Coulomb and Franklin Algorithm (CFA) was applied to select features in an intrusion detection system in cloud computing networks based on the Support Vector Machine (SVM). The proposed method was applied using the NSL KDD dataset, and the results were compared with the ensemble feature selection and grasshopper optimization algorithm (EFSGOA), the binary based particle swarm optimization algorithm (BPSO), and the standard and binary based particle swarm optimization algorithm (BPSO+SPSO). Performance measures The main ones used to evaluate the efficiency of the proposed algorithm are detection rate, accuracy, false alarm rate, and number of features identified. The results showed that the proposed method, which is better than the compared methods, enhanced the accuracy of intrusion detection in the CC system by 99.80%. In addition, it obtained low false alarm rates (0.0022) and only 17 features were selected from the raw data containing 41 features, which demonstrates the effectiveness of the proposed method.

KeyWords: Intrusion Detection System , Columb and Franklin Algorithm , Cloud Computing Network ,Optimization Algorithm ,Support Vector Machine Algorithm .

نظام كشف التسلل في الحوسبة السحابية باستخدام خوارزمية التحسين كولوم وفرانكلين مع آلة دعم المتجهات

إعداد

فاطمة عيسى خلف

إشرف

د. عمر الطراونة

الملخص

في ظل انتشار الحوسبة السحابية بسبب البيئة المفتوحة التي توفرها من خدمات وتطبيقات وموارد، اصبح لدينا كمية كبيرة من البيانات الحساسة والهامة التي يجب على مزودي السحابة توفير الامن والحماية لها من اي هجوم او عبث . ومن اكثر الطرق شيوعا لحماية البيانات هو استخدام نظام كشف التسلل IDS الذي يعتبر من خطوط الدفاع ، حيث يقوم بمراقبة حركة مرور البيانات عبر الشبكة لتحليل ومعالجة البيانات القادمة من الحوسبة السحابية CC للكشف عن اي سلوك اونشاط مشبوه لتحسين امن النظام . وتكون هذه البيانات بحاجة الى معالجة في الوقت الفعلي وبسبب كميتها الكبيرة سوف تؤدي الى نقص كفاءة IDS لاستغراقه وقت طويل في تحليل هذه الكمية من البيانات . لذلك قدم الباحثون العديد من الابحاث التي تتناول طرق واستراتيجيات لتحسين اداء IDS لحل هذه المشكلة. في هذه الاطروحة ، تم تطبيق خوارزمية كولوم وفرانكلين CFA لاختيار الميزات في نظام كشف التسلل في شبكات الحوسبة السحابية على اساس خوارزمية SVM . تم تقييم الطريقة المقترحة باستخدام مجموعة بيانات NSL KDD ، وتم استخدام الطرق التالية من اجل مقارنة النتائج خوارزمية تحسين الجندب (EFSGOA)،وخوارزمية تحسين سرب الجسيمات

ثنائي الاساس (BPSO)، وخوارزمية تحسين سرب الجسيمات على اساس قياسي وثنائي (BPSO+SPSO) من اجل قياس كفاءة واداء IDS من خلال قياس معدل الكشف، الدقة، معدل الإنذارات الكاذبة، وعدد الميزات المحددة. وأظهرت النتائج أن الطريقة المقترحة، زادت من معدل كشف التسلل في نظام CC بنسبة 99.77%. بالإضافة إلى ذلك، فقد قللت من معدل الإنذارات الكاذبة ومن عدد الميزات وكانت النتائج كما يلي على التوالي (0.0022) وتم اختيار 17 ميزة فقط من البيانات الأولية التي تحتوي على 41 ميزة، مما يدل على فعالية الطريقة المقترحة.

الكلمات المفتاحية : نظام كشف التسلل ، خوارزمية كولوم وفرانكلين ، شبكة الحوسبة السحابية، خوارزميات التحسين ، خوارزمية آلة دعم المتجهات .