هيكل وصول دقيق و آمن للبيانات الضخمة في بيئات التخزين السحابية

ندى معلث السحيمي

اشراف / د .فتحي عيسى

المستخلص

تستفيد العديد من الشركات والمؤسسات من خدمات التخزين السحابية لبناء منصات تحليل البيانات الكبيرة الخاصة بها، و تستخدم سياسات التحكم في الوصول لتقييد الوصول إلى البيانات الكبيرة الخاصة بالعملاء ونتائج التحليل المخزنة على السحابة. يعتبر أمازون أحد مقدمي خدمات التخزين السحابية الأكثر أهمية واستخداماً حسب الاحصائيات، و يستخدم سياسات تحكم بالوصول من النوع JSON ، حيث تعتبر صغيرة الحجم وسهلة الإنشاء والتخزين. من المتعارف عليه أن نجاح أي هجوم في اجراء تغييرات على ملفات التحكم بالوصول سيؤدي حتما إلى الوصول غير المسموح به إلى بيانات العملاء الكبيرة ونتائج التحليل و التي يمكن أن تكون ذات قيمة كبيرة. في هذه الأطروحة، نقترح نموذج أمني كفؤ ، رشيق و بسيط في نفس الوقت حيث يعتمد على التوقيع الرقمي كآلية حماية لتأمين سياسات التحكم بالوصول من النوع JSON. بإضافة التوقيع الرقمي إلى كل سياسة JSON فإننا سنمنع أي طرف غير شرعي، بما في ذلك مزود الخدمة من اجراء تغيير على سياسات التحكم بالوصول الخاصة بالعميل بطريقة غير مشروعة أو خلق سياسات جديدة بدون علم العميل، كما ستضمن سلامة وصحة السياسات المطبقة بالفعل بواسطة العميل.

قمنا بتنفيذ النموذج الأمني المقترح واختباره حيث اتضح أن الوقت المستهلك لإنشاء توقيع رقمي و التحقق منه لا يتجاوز بضع ثوان، كما لا يتطلب النموذج الأمني المقترح أي أجهزة خاصة ليتم تبنية فعلياً من قبل مزودي خدمات التخزين السحابية حيث أنه يعتمد كلياً على إضافة وظائف برمجية لإنشاء التواقيع الرقمية و التحقق منها ، أخيرا فإن النموذج الأمني المقترح يقدم الأمن لسياسات التحكم بالوصول مقابل الحد الأدنى من التكلفة المادية والجهد والوقت المستهلك.

SECURING ACCESS CONTROL POLICIES FOR BIG DATA ON CLOUD STORAGE

Nada Meleth Alsehaimi
Supervisor / Prof. Fathy Essa

ABSTRACT

Many companies and enterprises benefit from cloud storage services to build big data analysis platforms where Access Control Policies (ACPs) are used to restrict access to client's big data and analysis results stored on the cloud storages. Intuitively, any attack succeed in changing an ACP will inevitably lead to unauthorized access to the clients' big data and analysis results which could be of great value. In this thesis, we propose lightweight, efficient yet simple security modal depends on digital signature as a protection mechanism to secure ACPs of the format JSON used by Amazon Web Services (AWS) which is, according to statistics, the most popular cloud provider. Adding digital signature to each single JSON policy will prevent any illegitimate party, including the storage service provider, from illegally changing the client's ACPs or creating new policies without the client's knowledge; also it will ensure the integrity and authenticity of the ACPs applied by the client. We implemented prototype of our proposed security model using .NET Framework and tested it using sample consists of group of AWS policies. Results showed that the consumed time to create and verify digital signatures does not exceed few parts of a second, also the proposed security model does not require any additional hardware to be adopted by cloud storage providers as it depends entirely on adding programmatic functions to create and verify digital signatures. The proposed security model provides security for ACPs for minimum operational cost, effort and execution time.