Progetto di Architetture ed Algoritmi per la sicurezza di dati sensibili nel Cloud Computing pubblico

di ing. Fabio Bracci, assegnista "Antonio De Luca"

Descrizione del progetto

Il Cloud Computing è ritenuto ad una unanimità una tecnologia che rivoluzionerà la normale concezione di utilizzo del computer, portando vantaggiose funzionalità non solo ai clienti finali (quali assistiti, operatori sanitari, ecc.), ma anche alle software house che realizzano applicazioni per il Cloud Computing, definite Software as a Service (SaaS), quale Vitaever.

Tuttavia, alcuni componenti principali del Cloud Computing sono tutt'ora in una fase embrionale, ed inevitabilmente trascurano delle funzionalità fondamentali, come la sicurezza. Questa lacuna suscita una non totale fiducia a riguardo del Cloud rendendo la sua diffusione ed applicabilità più difficile.

All'interno del contesto dell'Assegno "Antonio De Luca", Nethical s.r.l. e l'Università degli Studi di Bologna, più precisamente con il Dipartimento di Informatica, Elettronica e Sistemistica (DEIS), hanno avviato un progetto di ricerca volto a studiare nuove soluzioni per rafforzare la sicurezza in ambiente Cloud per la protezione delle informazioni e il rispetto della normativa privacy.

La ricerca di meccanismi di protezione dei dati sensibili è stata svolta dall'Ing. Fabio Bracci, assegnista di ricerca "Antonio De Luca" presso il DEIS (Dipartimento di Informatica, Elettronica e Sistemistica), sotto la supervisione del Prof. Antonio Corradi e dell'Ing. Luca Foschini della Facoltà di Ingegneria dell'Università degli Studi di Bologna.

La fase iniziale del progetto è stata improntata su un accurato studio ed analisi di una piattaforma Cloud computing in sanità, in particolare focalizzando su quella Vitaever grazie alla disponibilità di dettagli tecnici offerti da Nethical, e sullo studio dello stato dell'arte mondiale sulle tecnologie di protezione dei dati in ambito Cloud. Come fonti si è utilizzato l'Institute of Electrical and Electronics Engineers [IEEE] e l'Association for Computing Machinery [ACM]), ma anche le normative vigenti (in ambito sanitario) rilasciate non solo dall'Unione Europea ma anche dallo standard attualmente in vigore negli USA (Health Insurance Portability and Accountability Act [HIPAA]).

La successiva fase è stata la progettazione di alcuni prototipi. Data la complessità e l'importanza, tale fase è stata suddivisa in due sottoproblemi:

1. Realizzazione di un meccanismo di cifratura dei dati sensibili: tutti i dati ritenuti sensibili, prima di essere memorizzati nel database, vengono cifrati utilizzando differenti chiavi di cifratura (cioè delle stringhe di caratteri simili a delle password) e resi quindi incomprensibili se non in possesso delle relative chiavi utilizzate per la cifratura;

2. Realizzazione di un meccanismo di salvataggio, recupero e ripristino delle chiavi di cifratura utilizzate per proteggere i dati: senza tali chiavi di cifratura, infatti, i dati non possono essere utilizzati.

Entrambi i problemi sono stati affrontati cercando sempre di utilizzare delle tecnologie standard, quale l'algoritmo di cifratura Advansed Encryption Standard (AES) e il Directory Server LDAP, per dotare il meccanismo di maggiore sicurezza e compatibilità.

Per quanto riguarda il primo sotto problema, l'Ing. Fabio Bracci è stato affiancato dalla laureanda Daniela Moschetto. Tra i principali compiti svolti in questa parte di progetto si annoverano:

- La gestione dell'autenticazione e dell'autorizzazione degli utenti (quali Assistiti, Medici, Operatori, ecc.) per abilitare il recupero e l'utilizzazione delle chiavi di cifratura;

- L'implementazione di un possibile algoritmo di cifratura e delle relative politiche di protezione (definizione dei campi sensibili, adozione di differenti chiavi di cifratura, ecc.).

Il prototipo realizzato è attualmente in fase di test.

Per quanto riguarda il secondo sotto problema, l'Ing. Fabio Bracci è stato affiancato dal laureando Jacopo Toccacieli. Il compito principale svolto in questa parte di progetto è indubbiamente la gestione, e quindi il salvataggio, il recupero ed il ripristino delle chiavi di cifratura.

Partendo da un servizio Open Source quale OpenLDAP, si sono realizzati degli script ad hoc per verificare il corretto salvataggio ed utilizzo delle chiavi di cifratura realizzando dei backup sia giornalieri che ad eventi (es: registrazione di un nuovo operatore). Grazie agli script realizzati è possibile ripristinare il servizio, in caso di perdita delle chiavi di cifratura, senza perdere alcuna informazione in caso di guasto.

Il progetto ha dunque portato ad una maggiore sicurezza nel trattamento dei dati sensibili, soprattutto in ambito Cloud pubblico, cercando di non impattare sulle prestazioni di un possibile sistema Cloud e cercando di non limitare la funzionalità tipicamente alta di un'interfaccia web.

Pubblicazioni

F. Bracci, A. Corradi, L. Foschini (2012). "Database Security Management for Healthcare SaaS in the Amazon AWS Cloud", fase di pubblicazione Institute of Electrical and Electronics Engineers (IEEE)

Seminari

MoCS2012 (http://mocs.deis.unibo.it/)

July 1st, 2012- Cappadocia, Turkey - Thursday 11:00-12:30

"Database Security Management for Healthcare SaaS in the Amazon AWS Cloud"
Fabio Bracci (University of Bologna, Italy); Antonio Corradi (University of Bologna, Italy); Luca Foschini (University of Bologna, Italy)