Павел Г. Герасимов,

ХИБРИДНИ ОБЛАЧНИ ТЕХНОЛОГИИ ОТ НОВО ПОКОЛЕНИЕ

Павел Г. Герасимов

Intellect TGK, Gate-92 DG, Sofia-Sevlievo, Bulgaria, p.g.gerasimov@gmail.com

***Abstract**: During the last 15 years, cloud architecture, and the based on it systems and technological solutions became fundamental parts of the global IT-ecosystem. The rapid and accelerated development of this technology, set many questions like "Do we know what types of dangers can expect in the cloud?, "How protected am I, my Organization, and the information stored on the cloud? "What means and methods should I use in order to protect myself and my information from attack on the cloud, and how to treat the consequences concerning me?", and "What the hybrid cloud can give me, that the standard can't?" In the following article, we will discuss some of the benchmarks in the nature of the cloud platforms, that could let us propose new type of Hybrid Cloud, and of course to present some new methods and solutions, for protecting the information on the cloud. In the end of the article, the reader will be able to understand a new type of hybrid cloud system, that gives the user the ability to control and manage the level of his protection, and to manage the risk concerning the storage of sensitive information on cloud storage.*

***Keywords**: Cloud, Hybrid Cloud, Protected Cloud Storage, Encryption, SECaaS, Cloud computing*

Въведение

По дефиниция облачната архитектура представлява тип специализирана компютърна услуга, предоставяна на потребителя чрез отдалечен компютър, към който потребителят се свързва посредством internet или специална комуникационна линия.

Националният Институт по Стандартизация и Технологии на САЩ (The National Institute of Standards and Technology - NIST) в своя бюлетин специално посветен на дефиницията на облачната архитектура дефинира четири основни модела на предоставената услуга: [1]

- **SaaS** ***(Software as a Service)*** – Софтуер като услуга или Приложно ниво (*Application layer*)
- **IaaS** ***(Infrastructure as a Service)*** – Инфраструктура като услуга или Хардуерно ниво (Hardware layer)
- **PaaS** ***(Platform as a Service)*** – Платформа като услуга или Междинно ниво (*Middleware layer*)
- **DaaS** ***(Database as a Service)*** – База данни като услуга.

През годините са се развили различни модели, в резултат на все по-разширеното използване на облачните услуги. В настоящата публикация ще се фокусираме върху една специфична форма, която е и предмет на теоретичните разглеждания.

С развитието на облачната архитектура, се достигна до четири базови структури:

- **Частен облак** *(Private Cloud)* – При него инфраструктурата на облака се притежава или наема от една организация и се използва само и единствено от нея.
- **Общностен облак** *(Community Cloud)* – Инфраструктурата на облака се споделя от няколко организации и служи за поддържането на специфична общност от потребители. Всички потребители споделят обща мисия, обща политика и общи изисквания към информационната сигурност.
- **Публичен облак** *(Public Cloud)* – Инфраструктурата на облака се притежава от една организация, която продава облачно-базирани услуги на широк спектър от клиенти.
- **Хибриден облак** *(Hybrid Cloud)* – При този тип архитектура, инфраструктурата на облака е съчетание от горе-представените три решения, които остават разграничими на база вътрешна политика за сигурност. В същото време те са свързани посредством стандартизирана или авторска технология, използвана от компанията провайдер.

В настоящата публикация, ще разглеждаме модификация на типа архитектура „Хибриден облак" и ще се опитаме да представим нови технически решения, към които този тип архитектура предполага.

Технико-икономическа обосновка

Според проучване на консултантската компания KPMG [2], около 25% от правителствата по света са насочили своя фокус за следващите 15 години към облачно-базираните системи и по-конкретно към разработка на хибридни системи с високо ниво на защита. Според посоченото проучване засиленият интерес се дължи основно на факта, че се налага значително оптимизиране на разходите по поддръжка на съществуващата IT-инфраструкура. В същото време изискванията за подобряване на общата сигурност, оптимизация на протоколите при реакция в случай на кибернетични атаки както и на противодействие на опитите за несанкциониран достъп до чувствителна информация все повече нарастват.

Отново, според същото проучване, все по-често на дневен ред се поставят въпроси касаещи защитеността на аутсорснатите информационни масиви, както и унификацията на методите за защита и тяхната междуплатформена съвместимост.

Друг много важен проблем е *зоната* (*територията*), на която се намират сървърите на компанията, поела дейността по обработка и защитено съхранение на информационните масиви. Проблемът е в резултат на тежката регионална и международна юридическа рамка, обхващаща функционирането на този вид технологични решения, както и на строгите процедури на сертификация по ISO.

Хибридният облак е изключително полезен и удобен за компании и държавни органи работещи с големи масиви от данни, изпитващи нужда от допълнителни системи за съхранение и обработка на информация, които нямат възможност да поддържат скъпоструваща IT-инфраструктура.

Съвременните хибридни облачни решения са изправени пред следните четири проблема [3, 4]:

- **Цена** – проблемът е свързан с необходимостта от наличие на локална сървърна инфраструктура при потребителя и отдалечен ресурс при провайдера на облачната услуга.
- **Режийни разходи** – енергийни разходи, вода, разходи за климатизация и вентилация, разходи за физическа сигурност и други.

- **Оперативни разходи** – свързани със системата на функциониране и обслужване на хибридния облак.
- **Амортизация** – важно е амортизацията да бъде отчетена като перо при поддръжката на хибридния облак, тъй като в зависимост от натовареността на системата трябва да бъдат прогнозирани с абсолютна точност периодите на обслужване на физическите устройства

Развитието на хибридните облачни решения, поставя въпроса за защитеността на информацията намираща се на тях и минимизиране на рисковете за потребителя на съответната услуга.

В течение на развитието на технологията се развива модела **SECaaS** – *(Security as a Service)* Сигурност като услуга. SECaaS предоставя на потребителя определен набор от инструменти, които подпомагат обезпечаването на неговата сигурност, както и инструменти за контрол на достъпа, инструменти за защита на информацията, защитени линии на достъп и други.

Използването на SECaaS има както свойте предимства така и някои недостатъци. [5]

Глобално погледнато за потребителя, облакът е „черна кутия", за която той няма информация от гледна точка на сигурността. Друг сериозен проблем е, че към момента степента на защитеност трудно може да бъде измерена, поради липса на утвърдена методология.

М.Карвало (M.Carvalho) в своя публикация от 2011, поставя въпроса за предоставяне на инструментариум на потребителя, посредством който той (*потребителят*) ще може да управлява защитата на информацията съхранявана на облака като по този начин се създава възможност за формиране на политики за определяне на риска.

Много е важно да отбележим, че SECaaS не е услуга, която може да се предоставя само на един потребител. Това е услуга предназначена за голям набор от потребители, както крайни, така и големи корпоративни структури.

Структура на Хибридния облак

Хибридните облаци като услуга са рискови, независимо от това, което се твърди за тях. На практика те са типични трислойни приложения, с всички произтичащи от това последствия.

Един от основните проблеми е, че контролът основно се извършва от административни структури, които обслужват сървърната част и бизнес слоя. В същото време клиентските приложения са мултифункционални и слабо защитени.

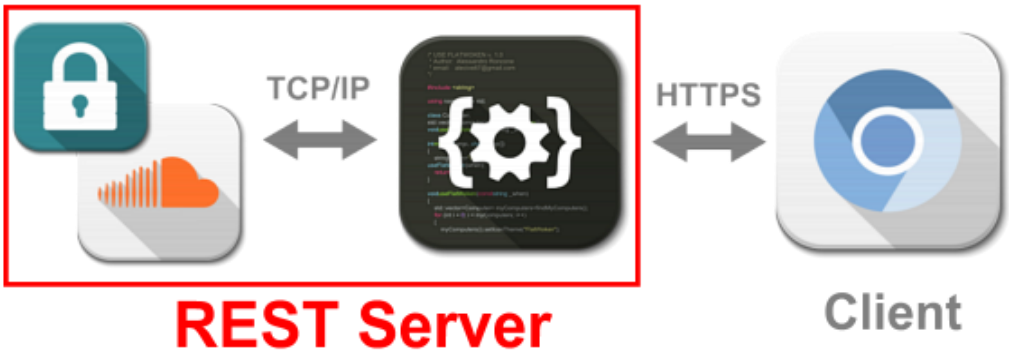
Поради тази причина е необходимо да се намери решение, което да позволи на крайните потребители да защитават използваната от тях информация, съобразно своите политики за сугурност, без това да нарушава общите правила за ползване на облака.

В зависимост от използвания клиент хибридните решения от ново поколение, могат да бъдат обособени в следващите три групи:

- **Web-базиран клиент** – Това са приложения, при, които като клиент за достъп се използва web-браузър. Този тип хибриден облак е достъпен под формата на internet-базирано хранилище. Това, което отличава този хибриден облак от други популярни алтернативи, съществуващи днес, е възможността потребителят да избира сам криптиращият механизъм за защита. Комуникацията с облака се извършва при използване на HTTP или FTP протокол. Управлението на жизнения цикъл на сесията се реализира при използване на TCP/IP проткол. Управлението се извършва от специализиран REST-сървър.
- **Специализиран клиент** – при тази реализация хибридният облак е достъпен посредством защитено крайно приложение. Този вид решения са извънбраузърни (*out of browser*), мултиплатформени решения, при които се елиминира частично или изцяло използването на HTTP протокол. Както и при web-базираните, така и тук потребителят може сам да избира криптографския алгоритъм, посредством който да защити своята информация. При този

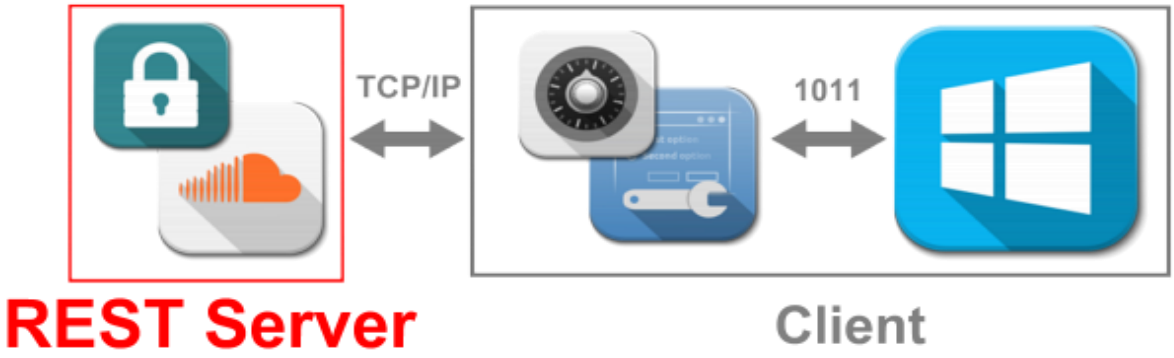
тип решение се извършва предварително криптиране от страна на потребителя. В този случай преносът е надеждно защитен дори тогава, когато не се използва VPN-канал или друго подобно решение.

-



Фигура: Схема на структурата на web-базирано приложение

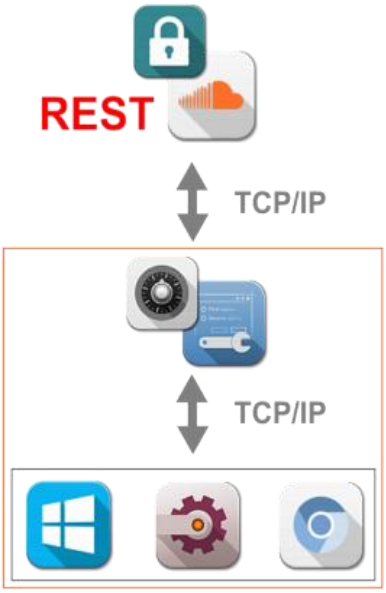
- **Специализиран клиент** – при тази реализация хибридният облак е достъпен посредством защитено крайно приложение. Този вид решения са извънбраузърни (*out of browser*), мултиплатформени решения, при които се елиминира частично или изцяло използването на HTTP протокол. Както и при web-базираните, така и тук потребителят може сам да избира криптографския алгоритъм, посредством който да защити своята информация. При този тип решение се извършва предварително криптиране от страна на потребителя. В този случай преносът е надеждно защитен дори тогава, когато не се използва VPN-канал или друго подобно решение.



Фигура 2: Използване на специализиран клиент

- **Специализирани решения (*специализиран пакет*)** – това е реализация на хибриден облак, подходяща за държавни и общински институции, малки и средни предприятия, обработващи големи масиви от разнородна информация (финасово-счетоводна, технологична, специализирана и др.) и нуждаещи се от гарантирана защита. Този потребителски пакет

позволява изграждане на нискобюджетна локална инфраструктура. Функционалността е аналогична на предходно описаните потребителски пакети.



Фигура 3: Трислойна хибридна структура.

Фигура 4: Двуслойна, хибридна структура

Защита на информацията съхранявана в хибридния облак

Както споменахме по-горе в нашите разглеждания, хибридният облак позволява както криптиране на информацията съхранявана на него така и криптиране от страна на крайния клиент. При трислойната архитектура това се извършва от бизнес слоя на приложението. При двуслойните решения механизът е различен.

Към самият хибриден облак е свързан специален оперативен модул, който е отговорен само и единствено за криптирането на съхраняваната информацията. Оперативният модул комуникира с

потребителя, като провайдера на услугата. Директната връзка оперативен модул-потребител, позволява на потребителя да поеме частично или напълно управлението на риска, свързан с отдаленото съхранение на информацията.

Контролът на жизнения цикъл за всяка една сесия се осъществява в реално време и се документира, съобразно действащите стандартни зисквания. За реализиране на този процес се използва контролен модул. При еднопроцесорните 32 разрядни апаратни решения се използва многопоточна обработка на данните. При многопроцесорните 64 разрядни се използва паралелна обработка.

Контролният модул на Хибридния облак следи за правилното разпределяне на изчислителните ресурси на облака, неговото дисково пространство и балансираното разпределение на заявките за обслужване, подавани от потребителите. Една от най-важните функции на контролът на сигурността (Information Security Control – ISC), който се изразява в превенция на опити за злонамерен достъп, DDoS – атаки, SQL – инжекции, нерегламентирано извличане на потребителски данни за достъп и други.

Друг важен аспект при реализацията на хибридни системи е възможността за автоматично изграждане на виртуални контейнери. За целта се използва специализиран by-pass механизъм., който изпълнява предпазна функция в случай на недопустимо натоварване на системата. В случай на невъзможност за обслужване на заявката се генерира виртуален контейнер, към който тя се пренасочва. Преди да бъде записана заявката се анализира и класифицира. Подредбата се извършва по приоритет, регламентиран от вътрешни правила. След като заявката бъде обработена, резултатът се съхранява в друг временен контейнер. При приключване на сесията двата виртуални контейнера се самоунищожават без да оставят остатъчна информация.

При специализираните пакети хибридният облак предоставя опцията за формиране на Защитено Работно Пространство (ЗРП).

Защитеното локално работно пространство има за цел да предостави на потребителя локално генериран виртуален контейнер, който да гарантира защитена среда за работа с чувствителна информация. В този случай информацията може да бъде прехвърлена към защитен облак или да бъде използвана като алтернативно решение за съхраняване на цифрови данни.

Фигура 4: Вътрешна структура на хибридния облак

При ЗРП данните се съхраняват в бинарен вид, като могат да бъдат частично или напълно криптирани. Физически ЗРП съществува до момента в който се осъществи пълна миграция на съхраняваната информация към хибридния облак и/или краен получател. Когато работната сесия приключи се извършва миграция или се задейства протокол за пълно унищожаване на данните.

За да бъдат предотвратени опити за несанкционирани действия от страна на неоторизирани потребители, процесът на миграция и унищожаването при ЗРП, е автоматизиран.

В случаите, когато се извършва миграция, системата прави проверка за наличие остатъчни елементи или електронни следи. Ако бъде констатирано наличието на такива автоматично се включва протокол за тяхното унищожаване.

При унищожаването на ЗРП се премахва всяка остатъчна информация. В този случай се генерира цифров маркер, който подготвя създаването на ново ЗРП, предназначено за изпълнението на нова задача.

Важно е да се отбележи, че хибридният облак и използването на ЗРП, гарантират надеждна анонимизация, а също така елиминират необходимостта от събиране на лични данни и тяхната последваща обработка и анализ.

Заключение

Хибридните облачни технологии са надеждна алтернатива на много изисквания, пред които са изправени съвременните системи за обработка и съхранение на информацията.

Все по-нарастващите регулации в сферата на защитата на личните данни, неизбежно ще доведат до излишно усложняване, а от там и до възникване на нови затруднения при проектирането и изграждането на системи за обработка, съхранение и трансфер на цифрова информация.

Анонимизацията на потребителите е компромисно решение. По този начин се създава баланс между нуждите на крайния потребител, нормативните разпоредби, финансовите ограничения и техническите решения, които съставляват една съвременна информационна система.

Абсолютизирането на сървърните технологии е подход, който води до нарастване на проблемите. От друга страна общият обем да данни расте, като това се случва най-вече в резултат на увеличаващият се информационен шум. Не бива да се забравя, че дейтацентровете са сериозни консуматори на електро енергия. Това поражда допълнителни проблеми, които към момента не се отчитат.

Хибридните решения са само една от възможните алтернативи. Все още има много въпроси, които чакат своя отговор, но бъдещето ще изисква един различен и по-гъвкав подход.

References

1. P. Mell and T.Grace, Sep-2011, “The NIST Definition of Cloud Computing.” National Institute of Standards and Technology
2. KPMG, “KPMG – Exploring the cloud – A global study of governments’ adoption of Cloud.”
3. Koushik Annapu reddy, “Security Challenges in Hybrid Cloud Infrastructures”, Aalto University – School of Science and Technology
4. Philipp C. Heckel “Hybrid Clouds: Comparing Cloud Toolkits”
5. M. Carvalho, 2011, “SECaaS – Security as a Service”, Inf. Syst. Secur. Assoc., vol.9, no.10.pp. 20-24
6. Adrian Yanes, “Reputation in Cloud Computing”, Aalto University, School of Science and Technology
7. Nedzelský R., “Hybrid cloud computing: Security Aspects and Challenges”, University of Economics Prague