УДК 004.056:061.68

МЕТОД МОДЕЛИРОВАНИЯ МАРШРУТОВ РАСПРЕДЕЛЕНИЯ ОБРАБОТКИ КРИТИЧНЫХ ДАННЫХ В ГИБРИДНОЙ СРЕДЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ МОДИФИЦИРОВАННЫХ СЕТЕЙ ПЕТРИ

А.В. Царегородцев, Е.А. Дербин, И.Н. Мухин

Использование облачных вычислений при построении ИТ-инфраструктуры организации подразумевает отказ организации от прямого контроля над аспектами безопасности. Возникает необходимость в решении задачи обеспечения конфиденциальности данных при проектировании архитектуры, основанной на технологии облачных вычислений. В статье рассматривается метод моделирования процесса обработки данных с помощью сетей Петри на основании требований политики безопасности организации, позволяющий получить важную информацию о структуре многоуровневой системы управления доступом в гибридной облачной сред

Ключевые слова: информационная безопасность, облачные вычисления, политика безопасности, система управления доступом, сети Петри

Преимущества облачных вычислений позволяют существенно сократить сроки и издержки на разработку и эксплуатацию информационных систем для организаций всех форм собственности. Но многие из функций, которые делают облачные вычисления такими привлекательными, могут вступать в противоречие с традиционными моделями обеспечения информационной безопасности. Принимая во внимание парадигму облачных вычислений, организация отказывается от прямого контроля над многими аспектами безопасности. При анализе сложных бизнес процессов в облачных средах очень трудно определить факт соответствия текущих полномочий субъекта к объекту доступа с соответствующим уровнем секретности.

В связи с этим возникает необходимость в разработке системного подхода на основе сетей Петри.

Царегородцев Анатолий Валерьевич – Институт информационных наук и технологий безопасности РГГУ, д-р техн. наук, профессор, e-mail: academic_tsar@mail.ru

Дербин Евгений Анатольевич - Институт информационных наук и технологий безопасности РГГУ, д-р воен. наук, доцент, e-mail: evg.derbin@yandex.ru

Мухин Илья Николаевич - Институт информационных наук и технологий безопасности РГГУ, доцент, e-mail: ilyuha1999@mail.ru

Такой подход позволяет исследовать процесс обработки данных с целью определения соответствия с утверждённой политикой безопасности организации в условиях гибридной среды облачных вычислений. Определим в рамках политики безопасности множество субъектов безопасности T и множество объектов O, функцию безопасности f, которая для каждого объекта и субъекта определяет принадлежность уровня безопасности $l \in L$, где $(L, \leq)$ структура вида $f: S \cup O \rightarrow L$ [1].

Проведём анализ распределения потока критичных данных в рамках среды облачных вычислений. Действия над данными отобразим в виде переходов сети Петри таким образом, что выполнение задачи связано с осуществлением перехода, вследствие которого появляется маркировка сети. На рис. 1 данные o_1,…, o_4 и отношения между ними (стрелочки) изображены в виде пунктирной линии (поток данных). Управляющий поток показан в виде сплошной линии (данные типа p_1,…, p_6 и их переходы). Выполнение задачи требует наличия маркёра, передаваемого с данными, на входной позиции t и приводит к созданию маркёра в выходной позиции t. Т.е. при выполнении задачи t доступ на чтение данных определяется наличием входного маркера, доступ на запись данных – выходного маркера. На рис. 1 конечное состояние процесса является *достижимым*.

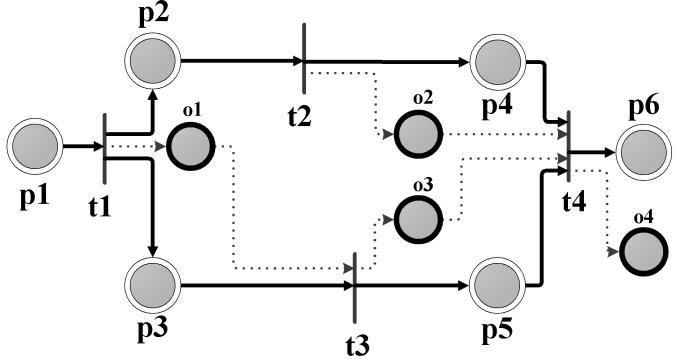

Рис. 1. Процесс обработки данных, представленный в виде сети Петри

Рассмотрим пример, когда облачный сервис на вход получает данные o_1, o_3 и производит данные o_4. В этом случае субъект политики безопасности должен иметь доступ на чтение данных o_1 и o_3 и доступ на запись данных o_4. Тогда субъект T должен иметь возможность читать все данные с маркером $\bullet t$ и записывать данные с маркером $t\bullet$, если для субъекта T и элементов в области $\bullet t \cup t\bullet$ присвоены соответствующие уровни доступа в соответствие с требованиями политики безопасности организации. Выполнение процесса обработки данных должно контролироваться управляющим элементом, который создаёт различные варианты развёртывания процесса обработки данных. Определим субъекты безопасности, как $T = \{t_1, t_2, t_3\}$, элементы данных $O = \{o_1, o_2, o_3, o_4\}$, элементы управления $P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, задачи/переходы $T = \{t_1, t_2, t_3, t_4\}$, для начальной позиции $M(p_1) = 1$, другие маркировки для неё равны 0.

На рис. 2 изображено 6 состояний процесса обработки данных в виде узлов.

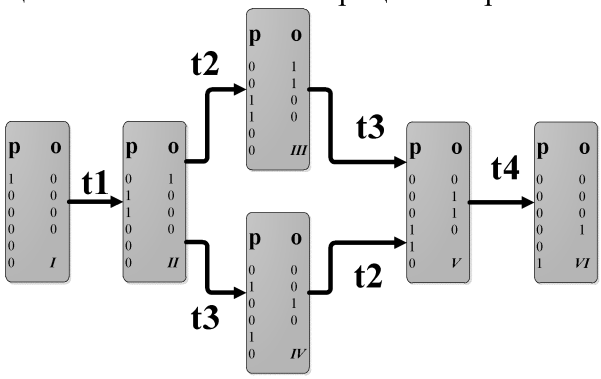

Рис. 2. Состояния процесса обработки данных

Каждое состояние характеризуется двумя столбцами: первый из столбцов (p) отражает состояние потока управления, второй (o) – состояние потока данных. Например, узел V имеет маркеры для данных $\{p_4, p_5\}$ (левый столбец узла V), $\{o_2, o_3\}$ (правый столбец узла V).

Примем во внимание требования политики безопасности «*» и «ss» модели доступа Белла-ЛаПадула [2]. Для рассматриваемого примера определим шкалу уровней информационной безопасности, состоящую из двух уровней: «Секретно» и «Несекретно». Присвоим уровни безопасности для субъектов рассматриваемого процесса, так, что все задачи будут наследовать полномочия роли, под которыми они выполняются (таблица 1).

Табл. 1

Уровни доступа облачных сервисов

Функция безопасности	Уровень ИБ
$f(t_1) = f(t_2) = f(t_4)$	Низкий (Несекретно)
$f(t_3)$	Высокий (Секретно)

Принципы построения сети Петри по требованиям безопасности, представим в виде следующих положений.

- Если субъект (облачный сервис) имеет высокий уровень доступа, то:

– разрешается совершать переход от узла N к узлу M, в результате которого происходит запись данных с высоким уровнем секретности;

– разрешается совершать переход от узла N к узлу M, в результате которого происходит чтение данных высокого или низкого уровней секретности;

– запрещается совершать переход от узла N к узлу M, в результате которого происходит запись данных низкого уровня секретности.

- Если субъект (облачный сервис) имеет низкий уровень безопасности, то:

– разрешается совершать переход от узла N к узлу M, в результате которого происходит запись данных с высоким или низким уровнем секретности;

– разрешается совершать переход от узла N к узлу M, в результате которого происходит чтение данных низкого уровня секретности;

– запрещается совершать переход от узла N к узлу M, в результате которого происходит чтение данных высокого уровня секретности.

На базе данных принципов формируется граф, который учитывает присвоенные уровни доступа всех субъектов рассматриваемого процесса и в зависимости от полномочий принимается решение о маркировке данных (рис. 3). Рис. 3 состоит из 15 узлов, которые показывают возможные маркировки обрабатываемых данных в сети Петри. Значения первого столбца показывают маркировку потока управления $p_1, p_2, p_3, p_4, p_5\, p_6$, значения второго – маркировку потока данных с соответствующими уровнями секретности для o_1, o_2, o_3, o_4. Например, узел XI имеет две управляющие метки данных p_2, p_3, метку данных с высоким уровнем безопасности o_3, метку данных с низким уровнем безопасности o_2.

Для наглядности будем использовать различные цвета для каждого узла.

1. Узлы, в рамках которых происходит обработка критичных данных, раскрашены в красный цвет и соответствуют компоненту частной среды облачных вычислений.

2. Узлы, в рамках которых происходит обработки несекретных данных, раскрашены в зеленый цвет. Данные узлы можно развернуть на общедоступной среде облачных вычислений, которая имеет более низкую стоимость, чем частная.

Построенная сеть Петри имеет два вида управляющих стрелок: *сплошная линия* используется для описания маркировки, где отсутствуют нарушения требования «*» и «ss»; *пунктирная линия* описывает маркировку данных, нарушающую одно из требований политики безопасности.

Выборочно приведём примеры нарушения политики безопасности построенного графа (наличие пунктирной линии) на рис. 3.

- Переход от состояния *II* к состоянию *VI* нарушает требование «*ss*» (принцип №3), т.е. запрещается совершать переход от узла *N* к узлу *M*, в результате которого субъектом с высоким уровнем безопасности (t_3) инициируется запись данных низкого уровня секретности (o_3).

- Переход из состояния *XII* в состояние *XV* нарушает требование «*» (принцип №6), то есть запрет чтения информации с высоким уровнем секретности o_2, o_3 субъектом с более низким уровнем безопасности (t_4).

Анализ рисунка 3 показывает, что не существует маршрута, который полностью удовлетворяет требованиям безопасности и делает возможным переход из состояния *I* в состояние *XIV* или *XV*. Для данного примера требования «ss» и «*» оказались невыполнимыми.

Можно рассмотреть разные варианты решения полученной проблемы. В частности, адаптировать текущую сеть Петри и включить в неё новые элементы. Введение в модель демилитаризованных зон, роль которых могут выполнять частные облака, позволит построить маршрут, выполнение которого выполнит основное требование *достижимости* сети Петри.

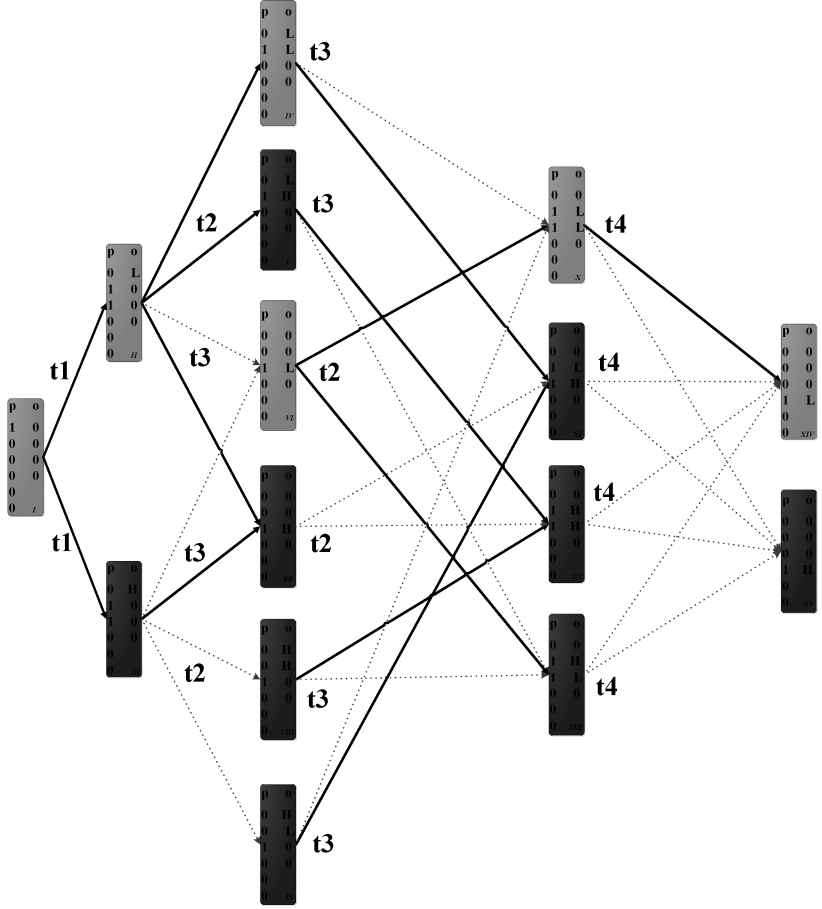

Рис. 3. Сеть Петри с присвоенными уровнями секретности для данных и сервиса

Предлагаемый подход к моделированию процесса обработки критичных данных на основе сетей Петри может служить основой для выбора оптимального варианта распределения обработки критичных данных между общедоступным и частным облаком.

Литература

1. Царегородцев, А.В. Один из подходов к управлению информационной безопасностью при разработке информационной инфраструктуры организации [Текст] / Царегородцев, А.В., Качко, А.К. // Национальная безопасность. – М.: Изд-во "НБ Медиа", № 1(18), 2012 г. С. 46-59.

2. Bell, D.E. and LaPadula, L.J. Secure Computer System: Unified Exposition and Multics Interpretation [Текст] / Tech report ESD-TR-75-306 // Mitre Corp, Bedford, 1976. 384 p.

ФГБОУ ВПО «Российский государственный гуманитарный университет»
Russian state university for the humanities

SIMULATION METHOD OF THE PROCESS ROUTE CRITICAL DATA IN A HYBRID CLOUD COMPUTING ENVIRONMENT BASED ON A MODIFIED PETRI NETS

A.V. Tsaregorodtsev, E.A. Derbin, I.N. Mukhin

The use of cloud computing to build of IT-infrastructure of the organization implies the refusal of the organization direct control over the security aspects. There is a need for solving the problem of data privacy in the design architecture based on cloud computing technology. In the article the simulation method of data processing using Petri nets based on the requirements of organization's security policy are considered. Such approach allows to obtain important information about the structure of multi-level access control system in a hybrid cloud environment

Key words: information security, cloud computing, security policies, access control system, Petri nets