УДК 004.056

Я. А. Бекенева, А. В. Дорохов
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Формальные модели систем распределенных вычислений и типы сетевых атак на них

Разработаны формальные модели систем облачных вычислений как одной из составляющих систем распределенных вычислений с целью дальнейшего их применения в системах имитационного моделирования. Представлены наиболее распространенные компьютерные модели облачных систем. Рассмотрены основные типы сетевых атак на системы облачных вычислений.

Системы облачных вычислений, атаки на системы облачных вычислений, формальные модели облачных вычислений, механизмы защиты

Распределенные вычисления предназначены для решения трудоемких вычислительных задач и осуществляются с помощью компьютеров, объединенных в вычислительную систему. Выделяют различные типы распределенных вычислений, наибольшее распространение среди которых получили облачные вычисления. В настоящее время вместе со стремительным ростом облачных вычислений возрастает и объем обрабатываемых данных. Под облачными вычислениями понимается тип параллельных и распределенных систем, состоящих из множества взаимосвязанных виртуальных компьютеров, которые предоставляются динамически и представлены в виде одного или нескольких унифицированных вычислительных ресурсов, основанных на соглашениях об уровне обслуживания, установленных посредством переговоров между поставщиком услуг и потребителями [1].

Повышение требований к сервисам облачных вычислений создает конкуренцию по предоставлению данной услуги. Это заставляет производителей расширять спектр предлагаемых сервисов облачных вычислений, повышая таким образом архитектурную и программную сложность систем. Повышение сложности систем влечет за собой увеличение числа их возможных уязвимостей. Очевидно, что массовая передача ресурсоемких задач в среду облачных вычислений в наступающем году вызовет появление большого количества злоумышленников в данной сфере. Другая важная причина состоит в накоплении огромного количества информации и вычислительных ресурсов в одном месте, из-за чего становится проще выкрасть данные пользователя или блокировать доступ к вычислительным ресурсам. В настоящее время многие провайдеры облачных вычислений заинтересованы в защите данных пользователей, но очень мало внимания уделяется устойчивости инфраструктуры облачных систем к атакам, что представляет собой угрозу для их существования в будущем.

Проблема улучшения стандартов безопасности и механизмов защиты систем является одной из наиболее актуальных на сегодняшний день. Для разработки и выявления эффективных методов защиты необходимо проводить множество экспериментов, имитирующих различные ситуации и типы атак. Это трудноосуществимо и затратно, если использовать реальные облачные системы, поэтому целью проекта является развитие моделей, методов и алгоритмов для исследования механизмов защиты облачных систем.

В настоящее время широко используются некоторые имитационные модели систем облачных вычислений.

CloudSim [2] разработан на основе системы GridSim в лаборатории GRIDS университета Мельбурна (Австралия). Разработанная система моделирования позволяет имитировать системы облачных вычислений, в частности компоненты, отвечающие за построение облачной инфраструктуры. CloudSim является самостоятельной платформой, которая позволяет моделировать датацентры, сервис-брокеры и различные политики доступа для широкомасштабных систем облачных вычислений.

iCanCloud [3] – это платформа имитационного моделирования для имитации систем облачных вычислений с основным упором на работу пользователей в таких системах. Основное предназначение iCanCloud – соотнести стоимость выполнения тех или иных приложений на определенном оборудовании, дать понять пользователю, какие затраты он понесет при этом.

Платформа GreenCloud [4] разработана с целью минимизировать потребление электрической энергии всеми составляющими системы, в особенности вычислительными серверами, сетевыми коммутаторами и линиями связи. Модель отслеживает общее потребление энергии обслуживания пользовательских запросов, характеризуясь при этом высокой производительностью.

Описанные ранее модели позволяют изучить различные характеристики облачных систем, однако ни одна из них не предназначена для тщательного исследования сетевой безопасности. В данной статье описываются формальные модели систем облачных вычислений и наиболее актуальные атаки на такие системы.

Системы облачных вычислений, как и любые компьютерные сети, представляют собой совокупности компьютеров, маршрутизаторов и каналов связи. Одним из основных вопросов моделирования компьютерной сети является моделирование ее топологии. Сетевая топология определяет расположение узлов и связи между ними. Интернет как объединение сетей имеет иерархическую структуру [5]. Модель компьютерной сети можно представить в виде кортежа:

$$N = < T, \mathrm{TP}, \mathrm{TR} >,$$

где T – тип топологии; TP – топология сети, TR – трафик в сети.

Топология сети включает в себя узлы (хосты) вычислительной сети и связи между ними.

Элементы множества H узлов (хостов) вычислительной сети представляются в виде

$$H = < \mathrm{Hwr}, \mathrm{Swr} >,$$

где Hwr – аппаратное обеспечение; Swr – программное обеспечение.

Аппаратное обеспечение включает в себя процессор, оперативную память, ресурсы для хранения данных и сетевые ресурсы. В облачных системах физические ресурсы абстрагируются от виртуальных и могут быть поделены между несколькими конечными пользователями и операционными системами без взаимных помех*.

Программные ресурсы могут быть описаны в виде кортежа:

$$\mathrm{Swr} = < \mathrm{Hyp}, \mathrm{VM}, \mathrm{SM} >,$$

где Hyp – гипервизор; VM – виртуальная машина; SM – сервисная модель.

Виртуальная машина включает в себя $\mathrm{VM} = < \mathrm{OS}, \mathrm{USW} >$, где OS – операционная система; USW – программное обеспечение пользователя.

Обычно выделяют 3 сервисные модели облачных вычислений, которые объединяются на уровне конечного пользователя*:

$$\mathrm{SM} = < \mathrm{SS}, \mathrm{PS}, \mathrm{IS} >,$$

где SS – SaaS (программное обеспечение как услуга); PS – PaaS (платформа как услуга); IS – IaaS (инфраструктура как услуга).

Software-as-a-Service (SaaS) – «Программное обеспечение как услуга» – уровень, который позволяет пользователю использовать программное обеспечение, предлагаемое провайдером. Для получения доступа необходимо лишь подключиться к Интернету с любого устройства, имеющего веб-браузер.

Модель SaaS включает в себя следующие компоненты:

$$\mathrm{SS} = < \mathrm{App}, \mathrm{CRM}, \mathrm{SocNet}, \mathrm{Strg} >,$$

где App – приложения; CRM – система управления взаимоотношениями с клиентами; SocNet – социальные сети; Strg – хранение данных пользователя.

Platform-as-a-Service (PaaS) – «Платформа как услуга» – уровень, на котором размещаются как приложения, предлагаемые провайдером, так и разрабатываемые пользователем. Платформа предоставляет как открытые языки программирования, так и собственные, набор необходимых базовых услуг для облегчения связи и мониторинга.

Модель PaaS может быть представлена в виде

$$\mathrm{PS} = < \mathrm{Lib}, \mathrm{Frm}, \mathrm{Lng}, \mathrm{Srv}, \mathrm{Tls} >,$$

где Lib – библиотеки; Frm – фреймворки; Lng – языки программирования; Srv – сервисы; Tls – инструменты.

Infrastructure-as-a-Service (IaaS) – «Инфраструктура как услуга» – предоставляет вычислительные ресурсы, ресурсы для хранения данных и каналы обмена данными, которые позволяют существующим и новым приложениям функционировать в облачной среде.

Модель IaaS может быть представлена как совокупность элементов:

$$\mathrm{IS} = < \mathrm{Ws}, \mathrm{Dtb}, \mathrm{Fwl}, \mathrm{LB} >,$$

* Eeva Savolainen Cloud Service Models. University of Helsinki, Finland, 2012. http://www.cs.helsinki.fi/u/epsavola/seminaari/Cloud%20Service%20Models.pdf

где Ws – веб-серверы; Dtb – базы данных; Fwl – межсетевые экраны; LB – распределители нагрузки.

Связи L между узлами вычислительной сети в контексте различных протоколов определяются связями между двумя соседними узлами и маршрутом, который проходит пакет данных для достижения узла назначения.

Трафик TR определяется в виде

$$\mathrm{TR} = \cup p_i^P,$$

где p_i – пакеты трафика; P – протокол, который используется для передачи пакета p ($p_i = \{\mathrm{Par}_i\}$, Par – параметры пакета в соответствии с используемым протоколом [5]).

Протокол P является программным и (или) аппаратным компонентом, реализующим набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами. Протокол реализует функцию трансляции сообщений при передаче их между подсистемами различного уровня в соответствии с сетевой моделью OSI*. Протоколы могут последовательно использовать друг друга, образуя структуру, состоящую из нескольких уровней. Модель протокола может быть записана как

$$P = \left\langle \begin{matrix} \mathrm{Phlev, DLlev, Netlev, Trlev,} \\ \mathrm{Seslev, Preslev, Applev} \end{matrix} \right\rangle,$$

где Phlev – физический уровень; DLlev – канальный уровень; Netlev – сетевой уровень; Trlev – транспортный уровень; Seslev – сессионный уровень; Preslev – уровень представления; Applev – прикладной уровень.

Как и любые вычислительные сети, облачные системы подвержены различным атакам. Модели атак на системы облачных вычислений можно описать множеством [6]:

$$\mathrm{ClAt} = \langle \mathrm{DDoS, CMIA, SCA, AuthAt, MITM...}n \rangle,$$

где DDoS – распределенная атака типа «отказ в обслуживании»; CMIA – внедрение вредоносного объекта; SCA – атаки по сторонним каналам; AuthAt – атаки при аутентификации; MITM – криптографическая атака типа «человек в середине». Данный перечень типов атак не является всеобъемлющим, так как появляются все новые и новые типы сетевых атак, в том числе представляющих угрозу и для систем облачных вычислений.

Опишем теоретико-множественную модель DDoS-атаки как одной из самых распространенных и в то же время опасных и разрушительных атак на компьютерную инфраструктуру [5]. Модели DDoS-атак генерируют события, используя нормальную функцию распределения, где ее значение определяет пользователь. Распределенные DoS(DDoS)-атаки на облачные приложения могут вызвать нехватку ресурсов как на виртуальных (например, атаки внутри сети VLAN), так и на физических устройствах. В первом случае это приведет к отказу в обслуживании отдельных пользователей, во втором – к отказу в обслуживании тысяч пользователей, чьи виртуальные компьютеры работают на физическом устройстве, подвергшемся атаке.

Модель DDoS можно описать так:

$$\mathrm{DDoS}_n = \langle I, \mathrm{TDD, NP,}\ f, \mathrm{Sprt, Dad, Dprt} \rangle,$$

где I – идентификатор атаки; TDD – тип DDoS-атаки; NP – количество отправляемых пакетов (определяет число пакетов, которое необходимо отправить на атакуемый узел); f – число пакетов, генерируемых в секунду. Параметр f и NP определяют длительность атаки $T_{\mathrm{Attack}} = \mathrm{NP}/f$; NA – параметр недоступен; Sprt – сетевой порт, с которого отсылаются пакеты; Dad — адрес назначения (IP-адрес компьютера-жертвы); Dprt – сетевой порт, на который отсылаются пакеты.

Внедрение вредоносного объекта заключается в том, что злоумышленник либо помещает в облачную систему виртуальную машину, которой он может управлять и тем самым влиять на работу всей облачной системы, либо внедряет вредоносный код в какие-либо программы. Этот тип атак формально может быть описан так:

$$\mathrm{CMIA} = \langle \mathrm{MI, AcM, Cont} \rangle,$$

где MI – внедряемый вредоносный объект (программный код или виртуальная машина); AcM – методы доступа для внедрения вредоносного объекта; Cont – управление внедренным вредоносным объектом.

Атаки по сторонним каналам заключаются в том, что вредоносная виртуальная машина помещается в непосредственной близости к целевому серверу облачной системы и осуществляет прослушивание канала связи, а в некоторых случаях – воздействие на компоненты системы. Атаки по сторонним каналам могут быть описаны следующим образом:

$$\mathrm{SCA} = \langle \mathrm{Ctl, AcSM, AnM, FlM} \rangle,$$

* ISO/IEC standard 7498-1:1994, International Organization for Standardization. Switzerland, 1994. www.iso.org

где Ctl – контроль над вычислительным процессом; AcSM – способы доступа к системе; AnM – методы анализа; FlM – способы воздействия на систему.

Основной целью атак на аутентификацию является получение логинов и паролей учетных записей пользователей. Такие атаки можно представить как совокупность следующих компонентов:

$$\mathrm{AuthAt} = \langle \mathrm{AcntM}, \mathrm{NLAM} \rangle,$$

где AcntM – способы перехвата данных учетных записей пользователей; NLAM – методы нелегитимной аутентификации.

Атаки типа «человек в середине» заключаются в том, что при обмене данными между двумя пользователями сети все передаваемые пакеты проходят через третье лицо, которое может не только видеть содержание сообщений, но и изменять его. Атаки такого типа могут быть представлены так:

$$\mathrm{MITM} = \langle \mathrm{PaC}, \mathrm{CrypM} \rangle,$$

где PaC – способы перехвата пересылаемых пакетов; CrypM – способы шифрования.

В данной статье были рассмотрены модели систем облачных вычислений с точки зрения теоретико-множественного подхода, а также были представлены наиболее распространенные атаки на облачные системы. Очевидно, что для повышения безопасности систем облачных вычислений необходимо совершенствовать механизмы защиты. В будущих работах планируется рассмотреть механизмы защиты систем облачных вычислений от сетевых атак различного вида. В дальнейшем представленные ранее формальные модели будут реализованы с помощью методов компьютерного моделирования с целью наиболее детального изучения уязвимостей облачных систем и создания оптимальных методов их защиты.

Работа выполнена в СПбГЭТУ «ЛЭТИ» при финансовой поддержке Министерства образования и науки Российской Федерации в рамках договора № 02.G25.31.0058 от 12.02.2013 г.

СПИСОК ЛИТЕРАТУРЫ

1. Buyya R., Yeo C. S., Venugopal S. Market oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities // In Proc. of the 10th IEEE Intern. Conf. on High Performance Computing and Communications, China, 2008. P. 5–13.

2. Buyya R., Ranjan R., Calheiros R. N. Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities // Proc. of the 7th High Performance Computing and Simulation Conf., Leipzig, Germany, June 21–24, 2009. P. 1–11.

3. Covarrubias A. N., Castane G. G. iCanCloud: Quick guide, 2011. URL: http://www.arcos.inf.uc3m.es/~icancloud/iCanCloud_Quickguide.pdf

4. Garg S. K., Green R. B. Cloud computing and Environmental Sustainability. Cloud computing and Distributed Systems (CLOUDS) / Laboratory Dept. of Computer Science and Software Engineering. The University of Melbourne. Australia, 2011.

5. Котенко И. В., Шоров А. В. Механизмы защиты компьютерных сетей от инфраструктурных атак на основе биоинспирированного подхода «нервная система сети» // Вопр. защиты информации. 2013. № 2. С. 57–66.

6. Ajey Singh Dr. Maneesh Shrivastava Overview of Attacks on Cloud // Computing, Intern. J. of Engineering and Innovative Technology (IJEIT). 2012. Vol. 1, is. 4. P. 321–323.

Ya. A. Bekeneva, A. V. Dorokhov
Saint-Petersburg state electrotechnical university «LETI»

FORMAL MODELS OF DISTRIBUTED COMPUTING SYSTEMS AND TYPES OF THE ATTACKS ON THEM

In this paper the formal model of cloud computing systems as type of distributed computing systems are developed. The popular cloud simulators are presented. Network attacks on cloud computing systems are presented. In the future work the developed models will be applied in the simulation systems.

Cloud computing systems, attacks on cloud computing systems, formal model of cloud computing systems, defense mechanisms