МРНТИ 20.15.05

ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Жумашев Н.Ж., Кусепова Л.Т.
Международный университет Астана, Нур-Султан, Казахстан
e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Аннотация. Актуальность данного исследования состоит в том, что облачными системами в сегодняшние дни пользуются не только определенные группы пользователей, а также множество компаний применяют их как хранилище данных и используют для осуществления обмена данными. Облачные вычисления состоят из таких основных компонентов, как ядро платформы, интерфейс, хранилище данных, управление пользователями, функционирование приложений, которым обязательно нужно осуществлять мониторинг системы в целом и обеспечивать их защиту. Соответственно в данной статье было особое внимание уделено облачным вычислениям и их различным подходам обеспечения безопасности, а также методам шифрования данных, осуществляющим шифрование с симметричным и асимметричным ключами. Система облачных вычислений могут быть подвержены к различным угрозам безопасности, а именно угрозам конфиденциальности, целостности, доступности данных и облачной инфраструктуры.

Ключевые слова: облачные вычисления, безопасность, конфиденциальность, Docker, Kubernetes

Введение

Облачные платформы предоставляют свои ресурсы в виде сервисов, поддерживающих различные услуги, в которой обеспечиваются подходящей инфраструктурной поддержкой пользовательские приложения. Благодаря поддержке управления облачными приложениями осуществляется удобный доступ к аппаратно-программным платформам, т.е. вычислительным ресурсам в виде сетей, устройств хранения данных, приложений. В состав облачной платформы входит следующие основные компоненты:

Ядро платформы: осуществляет интеграцию облачных сервисов со средами и наборами утилит.

Интерфейс: пользователь через различные API и веб-интерфейсы взаимодействуют с облаком.

Хранилище данных: хранятся большие объемы данных.

Управление пользователями: оптимизируются и подстраивается под задачи пользователей.

Мониторинг функционирования приложений и их поддержка: осуществляется интеграция приложения с облачными сервисами.

Каждый из этих компонентов уязвим к программным или иным ошибкам, допущенными пользователями и сервисом.

Облачные вычисления имеют ряд преимуществ, которые побудили пользователей и клиентов перенести свои данные в облако, использовав при этом облачные серверы. Любая форма информации и данные клиентов загружаются на облачные сервера и могут быть сохранены на хранилище данных облачного провайдера, который предоставляет множество услуг. Соответственно вся информация и данные пользователей должны быть защищены и обеспечены безопасностью. Иначе это могло привести к утечке данных и получению несанкционированного доступа злоумышленниками.

Система облачных вычислений могут быть подвержены к различным угрозам безопасности, а именно угрозам конфиденциальности, целостности, данных и облачной инфраструктуры.

Обзор литературы

Актуальность данного исследования обусловливается тем, что облачные вычисления становятся неотъемлемой частью повседневной жизни каждого гражданина, также компаний, при этом возрастает необходимость обеспечения безопасности каждого компонента в моделях обслуживания и развертывания облачных сервисов. Для развертывания облачных вычислений и предоставления ресурсов пользователям применяются технологии виртуализации, контейнеризации и оркестровки. При виртуализации клиентам предоставляются виртуальные ресурсы, а контейнеризация упрощает виртуализацию за счет специальной конструкции контейнеров в виде пакетов приложений из отдельных образов.

В работе Серикулы О. [1] описываются потенциальные угрозы информационной безопасности в технологии виртуализации, к примеру, пользование общего хранилища данных разными виртуальными машинами. Виртуальные машины могут клонироваться и перемещаться между физическими серверами. Каждая виртуальная машина хранится в виде отдельных файлов и могут быть изменены по необходимости от нужд пользователя, т.е. уменьшение и увеличение размера разделов могут привести к изменению физических секторов и перемещению данных с одной виртуальной машины на другую.

В работе [2] рассматривается использование технологии контейнеризации при разработке программ. Самыми популярными технологиями контейнеризации являются Docker и Kubernetes. Безопасность Kubernetes основана на следующих принципах: облако, кластер, контейнер и код. Основой безопасности Kubernetes является базовая физическая инфраструктура. Защита кластера включает компоненты API и все приложения. При обеспечении безопасности контейнеров производится сканирование контейнеров на наличие уязвимостей во время сборки. Код является поверхностью для атаки любой среды Kubernetes и обеспечение его безопасности является главной необходимостью системы, регулярное тестирование и сканирование могут предотвратить возникновение проблем безопасности в данной среде.

В работе [3] криптография определяется решением множеств проблем, а именно он помогает обеспечивать конфиденциальность, целостность и доступность информации, т.е. преобразовывает данные из простой формы в зашифрованную. При шифровании и дешифровании используются ключи. По количеству ключей криптографию разделяют на криптосистемы с асимметричным ключом и с симметричным ключом [3]. К шифрам с симметричным ключом относятся DES, Triple DES, blowfish, AES, а к асимметричным – RSA, ElGamal, DSA. Они имеют как преимущества, так и недостатки. В зависимости от этого сейчас применяются гибридный криптографический подход.

В статье M. K. Sinchana and R. M. Savithramma [4] представили обзор по безопасности облачных вычислений. В работе были изучены набор гибридных криптографических моделей и их конструкция, описаны преимущества и реализация каждой модели. Тут же рассматривается повышение безопасности и его эффективность осуществляется комбинированием симметричными и асимметричными видами шифрования.

В [5] работе был выполнен сравнительный анализ шести различных работ, использующие схемы дедупликации для эффективного доступа к облачным серверам. В качестве основных параметров, учитывающих при измерении производительности были производительность записи, размеры фрагментов и использование оперативного запоминающего устройства. Дедупликация снижает нагрузки на сервер, обеспечивая при этом, безопасный доступ к данным и помогает избежать избыточности данных. В работах, рассмотренные в данной статье объединяют безопасность и дедупликацию, обеспечивающую высокую производительность с точки зрения использования энергии, скорости доставки пакетов и временной задержки [5].

В работе [6] определяет дедупликацию данных как ограничительного подхода для удаления идентичных документов с повторяющейся информацией в репозитории. Данный метод используется для увеличения репозитория и уменьшения полосы пропускания.

В работе [7] представлен алгоритм конвергентного шифрования для обеспечения безопасности данных в облачных вычислениях. Чтобы найти дубликат документа и провести анализ типа документа и его преобразования в байт используется анализ границ на уровне индекса. Если копия документа была отклонена, то на следующем уровне документ преобразовывается в формат шифрования с использованием конвергентного шифрования.

Управление безопасностью облачной среды постоянно интегрируется и изменяется, т.к. это обусловлено тем, что злоумышленники могут использовать уязвимости, вызванные впоследствии неправильных манипуляции пользователей или конфигурациями системы. Приспособляемость модели безопасности является критически важным требованием при рассмотрении ее для облачных сред [8].

Методы исследования

В данной работе был проведен анализ статей, рассматривающих безопасность облачных вычислений и изучены методы шифрования, AES, DES, 3DES, RSA и определены следующие параметры оценки, включающее время шифрования и дешифрования, пропускную способность и длину зашифрованного текста. Время процесса шифрования зависит от увеличения количества символов. Время процесса дешифрования показывает восстановление исходных данных по истечению какого-то промежутка времени. Вычислить его можно по следующей формуле:

$$Time = Time_{end} - Time_{start} \quad (1),$$

где Time означает потребляемое время, Timeend – время окончания и Timestart – время начала.

Эффективность алгоритмов обеспечения безопасности в облачных вычислениях можно проанализировать с помощью его пропускной способности. Пропускная способность алгоритма прямо пропорциональна производительности, т.е. чем выше производительность, тем выше пропускная способность [8]. Формула, которая рассчитывает пропускную способность методов шифрования, выглядит следующим образом:

$$Th = Size_{Plain\_text} / Time_{enc} \quad (2)$$

где Th означает пропускную способность, $Size_{Plain\_text}$ – размер обычного текста и $Time_{enc}$ – время кодирования.

При шифровании на стороне клиента данные шифруются перед загрузкой на сервер, а объем загруженных данных напрямую влияет на время передачи [9].

Защита сервисов облачных систем не ограничиваются шифрованием, также для этого необходим комплексный подход, предусматривающий весь жизненный цикл процессов облачных систем, зависимостей, межсервисных взаимодействий, вызовов внешних библиотек, уязвимости.

При рассмотрении безопасности облачных сервисов как SaaS, определяются характеристики поведения приложения и уязвимости системы. Приложения можно классифицировать по характеру поведения следующим образом: безопасный, вредоносный и уязвимый. Состояние приложения диагностируются с точки зрения потенциального риска, проверки поведения и угроз безопасности. Риск безопасности можно подразделить на критическую, высокую, среднюю и низкую. Для каждого

обнаруженного небезопасного потока уровень риска равен максимальному уровню безопасности его источника [10].

Результаты и обсуждение

В данной работе были исследованы вопросы организации и обеспечения безопасности в облачных вычислениях и нацелена на определение эффективности алгоритмов защиты облачных систем в целом. При диагностике безопасности нужно рассматривать его в соответствии с основными моделями облачных вычислений: в плане инфраструктуры как сервис (IaaS), платформы как сервис (PaaS) и программное обеспечение как сервис (SaaS). Защита сервисов облачных систем применяется комплексный подход, предусматривающий весь жизненный цикл процессов облачных систем, зависимостей, межсервисных взаимодействий, вызовов внешних библиотек и уязвимости.

Выводы

Рассмотрев вопросы организации и обеспечении безопасности в облачных вычислениях можно сделать вывод о нижеследующем:

- не рекомендуется разрешать реестрам и сомнительным службам работать в облаке;
- нужно следить за тем, чтобы никто не получил доступ к информации о кредитных картах и транзакциях;
- учетные данные для входа в облачную систему должны быть надежно защищены, механизмы обмена учетными данными должны быть установлены должным образом;
- соединения API между моделями обслуживания должны быть правильно установлены;
- критерии сетевой безопасности должны соответствовать уровню безопасности IaaS;
- нужно периодически выполнять сканирование уязвимостей и проверку настроек;
- шифровать данные, находящиеся на облачном сервисе;
- необходимо использовать двухфакторную аутентификацию для доступа в систему;
- необходимы комплексные процедуры безопасности и управления данными, т.е. выполнять дедупликацию данных.

Список литературы

[1] Серикулы О. Информационная безопасность при облачных вычислениях. Вестник магистратуры. 2019. 6-5(93).

[2] Мельникова А.Е., Рычков В.А. Использование технологии контейнеризации при безопасной разработке программного обеспечения. Материалы второго международного научно-практического форума по экономической безопасности «VII ВСКЭБ». – Москва, 2021.

[3] Murad Sh.H., Rahouma K.H. Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. Procedia Computer Science. 2021. 194. 165–172.

[4] Sinchana M. K., Savithramma R. M. Survey on Cloud Computing Security. In Innovations in Computer Science and Engineering. Springer, Singapore, 2020. 1-6.

[5] Pragash K., Jayabharathy J. A survey on DE – Duplication schemes in cloud servers for secured data analysis in various applications. Measurement: Sensors. 2022.

[6] Geeta C.M., Shreyas R.Ga. Raju, Raghavendra S., Rajkumar B., Venugopal K.R., Iyengard S.S., Patnaik L.M. SDVADC: Secure Deduplication and Virtual Auditing of Data in Cloud. Procedia Computer Science. 2020. 2225–2234.

[7] Krishnasamy V., Venkatachalam S. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings. 2021.

[8] Irsheida A., Murada A., AlNajdawia M., Qusef A. Information security risk management models for cloud hosted systems: A comparative study. Procedia Computer Science. 2022. 205–217.

[9] Thabit F., Alhomdy Sh., Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks. 2021. 18-33.

[10] Elsayed M., Zulkernine M. Offering security diagnosis as a service for cloud SaaS applications. Journal of Information Security and Applications. 2019. 32-48.

References

[1] Serikuly O. Informatsionnaya bezopasnost' pri oblachnykh vychisleniyakh. Vestnik magistratury. 2019. 6-5(93).

[2] Mel'nikova A.Ye., Rychkov V.A. Ispol'zovaniye tekhnologii konteynerizatsii pri bezopasnoy razrabotke programmnogo obespecheniya. Materialy vtorogo mezhdunarodnogo nauchno-prakticheskogo foruma po ekonomicheskoy bezopasnosti «VII VSKEB». – Moskva, 2021.

[3] Murad Sh.H., Rahouma K.H. Implementation and Performance Analysis of Hybrid Cryptographic Schemes applied in Cloud Computing Environment. Procedia Computer Science. 2021. 194. 165–172.

[4] Sinchana M. K., Savithramma R. M. Survey on Cloud Computing Security. In Innovations in Computer Science and Engineering. Springer, Singapore, 2020. 1-6.

[5] Pragash K., Jayabharathy J. A survey on DE – Duplication schemes in cloud servers for secured data analysis in various applications. Measurement: Sensors. 2022.

[6] Geeta C.M., Shreyas R.Ga. Raju, Raghavendra S., Rajkumar B., Venugopal K.R., Iyengard S.S., Patnaik L.M. SDVADC: Secure Deduplication and Virtual Auditing of Data in Cloud. Procedia Computer Science. 2020. 2225–2234.

[7] Krishnasamy V., Venkatachalam S. An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. Materials Today: Proceedings. 2021.

[8] Irsheida A., Murada A., AlNajdawia M., Qusef A. Information security risk management models for cloud hosted systems: A comparative study. Procedia Computer Science. 2022. 205–217.

[9] Thabit F., Alhomdy Sh., Jagtap S. A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. International Journal of Intelligent Networks. 2021. 18-33.

[10] Elsayed M., Zulkernine M. Offering security diagnosis as a service for cloud SaaS applications. Journal of Information Security and Applications. 2019. 32-48.

БҰЛТТЫ ЕСЕПТЕУЛЕРДІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ЖӘНЕ ҰЙЫМДАСТЫРУ

Жумашев Н.Ж., Кусепова Л.Т.
Астана Халықаралық университеті, Нұр-Сұлтан, Қазақстан
e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Аңдатпа. Бұл зерттеудің өзектілігі, бүгінгі таңда, бұлтты жүйелерді қолданушылардың белгілі бір топтары ғана емес, сонымен қатар көптеген компаниялар оларды деректер қоймасы ретінде және деректермен алмасу үшін пайдаланады. Бұлтты есептеулер платформа ядросы, интерфейс, деректер қоймасы, қолданушыларды басқару, қосымшалардың жұмыс жасауынан құралатын негізгі компоненттерден тұрады, сондықтан жүйені тұтастай мониторинг жүргізіп, олардың қорғалуын қамтамасыз ету керек. Тиісінше, осы мақалада бұлтты есептеулерге және оның әр түрлі қауіпсіздік тәсілдеріне, сондай-ақ симметриялық және асимметриялық кілттермен шифрлауды жүзеге асыратын деректерді шифрлеу әдістеріне ерекше назар аударылды. Бұлтты есептеу жүйесі әр түрлі қауіпсіздік қатерлеріне, атап айтқанда, құпиялылық, тұтастық, деректердің қолжетімділігі және бұлтты инфрақұрылым қауіптеріне ұшырауы мүмкін.

Кілттік сөздер: бұлтты есептеулер, қауіпсіздік, құпиялылық, Docker, Kubernetes

ORGANIZATION AND SECURITY OF CLOUD COMPUTING

Zhumashev N. Zh. , Kusepova L. T.
Astana International University, Nur-Sultan, Kazakhstan

e-mail: nurik.universal@gmail.com
https://orcid.org/0000-0002-7972-3169

Abstract. The relevance of this study lies in the fact that today not only certain groups of users use cloud systems, but also many companies use them as a data warehouse and use them to exchange data. Cloud computing consists of such basic components as the platform core, interface, data storage, user management, application operation, which must monitor the system as a whole and ensure their protection. Accordingly, in this article, special attention has been paid to cloud computing and its various security approaches, as well as data encryption methods that perform encryption with symmetric and asymmetric keys. A cloud computing system can be exposed to various security threats, namely confidentiality, integrity, data availability and cloud infrastructure threats.

Keywords: cloud computing, security, privacy, Docker, Kubernetes

Авторлар жайында мәлімет:

Қаз.: Жумашев Нурдаулет Жанибекулы - Астана халықаралық университетінің студенті, nurik.universal@gmail.com

Рус.: Жумашев Нурдаулет Жанибекулы - студент Международного университета Астана, nurik.universal@gmail.com

Англ. Zhumashev Nurdaulet Zhanibekuly - student of Astana International University, nurik.universal@gmail.com

Қаз.: Кусепова Лаззат Тұңғышбайқызы - Астана халықаралық университетінің аға оқытушысы, lazzatk@mail.ru

Рус.: Кусепова Лаззат Тұңғышбайқызы - старший преподаватель Международного университета Астана, lazzatk@mail.ru

Англ.: Kusepova Lazzat Tungyshbaikyzy - senior lecturer at Astana International University, lazzatk@mail.ru