УДК 004.62

Ахметов Р.Д.
студент магистратуры
кафедра “Информационных систем”
Тимергалин А.Р.
студент магистратуры
кафедра “Информационных систем”
Князев О.А.
студент магистратуры
кафедра “Информационных систем”
Набережночелнинский институт-филиал
Казанского Федерального Университета
Республика Татарстан, г. Набережные Челны

ОБЛАЧНАЯ КРИПТОГРАФИЯ

Аннотация: В данной статье рассматриваются основы облачной криптографии и методы её обеспечения. Также исследуются различные криптографические методы, используемые основными поставщиками облачных услуг.

Ключевые слова: криптография, шифрование, облачные вычисления, облачная криптография.

Akhmetov R.D.
student of magistracy
Department of Information Systems
Timergalin A.R.
student of magistracy
Department of Information Systems
Knyazev O.A.
student of magistracy
Department of Information Systems
Naberezhnye Chelny Institute-Branch
of Kazan Federal University
Republic of Tatarstan, Naberezhnye Chelny

CLOUD CRYPTOGRAPHY

Abstract: This article discusses the basics of cloud cryptography and how to support it. It also explores various cryptographic techniques used by major cloud service providers.

Key words: cryptography, encryption, cloud computing, cloud cryptography.

Облачные вычисления — это структура для предложения сетевого доступа по запросу к объединенному пулу конфигурируемых вычислительных ресурсов (например, сетей, серверов, хранилищ, программного обеспечения и услуг), которые могут быть быстро предоставлены и выпущены с ограниченными действиями по техническому обслуживанию или участием поставщика услуг[1]. В облачных вычислениях ресурсы абстрагируются и виртуализируются из IT-инфраструктуры поставщика облачных услуг и становятся доступными для клиентов. Облачная инфраструктура предоставляет различные преимущества потребителям облака и другим основным заинтересованным сторонам. Некоторые из этих преимуществ - доступ к данным, хранящимся в облаке, независимо от их местонахождения, оплата по запросу, а также экономические выгоды за счет избавления компании от покупки оборудования и другой IT-инфраструктуры[2]. Несмотря на все эти преимущества, облачные вычисления вызывают определенную озабоченность. Основное внимание в индустрии облачных вычислений уделяется безопасности[3]. Первое и наиболее очевидное беспокойство — это соображения конфиденциальности, так как потребитель не может быть абсолютно уверен в сохранности и безопасности своих данных, хранящихся в облаке. Поскольку в основе облачных вычислений лежит Интернет, данные, перенесенные в облако, могут быть получены кем угодно из любого места в случае проблем в системе безопасности. Хакеры могут пойти на любое преступление, чтобы скомпрометировать данные[4]. От продажи конфиденциальной информации конкурентам и тем, кто находится в скрытой сети (darknet), до шифрования вашего хранилища и данных в целях вымогательства, или они могут просто удалить что-либо, чтобы нанести вред вашей компании. Поскольку, если ваши данные хранятся на чужих компьютерах, вы являетесь зависимыми от мер безопасности, принимаемых другой стороной. Организации не имеют

особого контроля над тем, что происходит с их данными, поскольку все в облаке, включая безопасность, управляется поставщиком облачных услуг.

Защита данных в облаке.

Многочисленные преимущества облачных вычислений побудили многие организации и правительственные учреждения перенести свои данные в облако[2]. Это дает злоумышленникам возможность также использовать уязвимости в облачных вычислениях и нарушить безопасность облака. Подпитываемые различными программами, они могут нанести вред организациям путем кражи данных, выполнения атак типа «Man-in-the-Middle» и нарушения целостности данных. Многие облачные гиганты, такие как Google, Amazon и Microsoft, приняли различные меры для защиты данных, хранящихся на их облачных платформах, их клиентами[2]. Но данные должны быть защищены от несанкционированного доступа во всех трех состояниях данных (данные в состоянии покоя, данные в процессе передачи и данные в процессе обработки). Некоторые организации знают об этих проблемах безопасности и шифруют свои конфиденциальные данные перед их переносом в облако. Это обеспечивает еще один уровень безопасности передаваемых данных со стороны клиента.

Криптография.

Криптография — это наука, где объектами исследований являются методы обеспечения конфиденциальности данных, их целостности, аутентификации и шифрования. Передаваемые данные скрываются и отображаются в формате зашифрованного текста, который нечитаем и непонятен неавторизованному пользователю. Ключ используется для преобразования зашифрованного текста в простой текст. Этот ключ хранится в секрете, и только уполномоченные лица имеют к нему доступ. Шифрование - один из самых безопасных способов избежать атак MitM, потому что даже если передаваемые данные будут перехвачены,

злоумышленник не сможет их расшифровать. В облачной криптографии есть два основных типа алгоритмов шифрования. Это: симметричные и асимметричные алгоритмы шифрования.

Алгоритмы симметричного шифрования (криптография с секретным ключом).

Алгоритмы симметричного шифрования использует один ключ как для шифрования, так и для дешифрования. Примеры этих алгоритмов шифрования кратко описываются ниже.

Стандарт шифрования данных (DES).

DES — это стандарт шифрования данных, который использует единый секретный ключ как для шифрования, так и для дешифрования. Он использует 64-битный секретный ключ, 56 бит которого генерируются случайным образом, а остальные 8 бит используются для обнаружения ошибок. Он использует алгоритм шифрования данных (DEA), секретный блочный шифр, использующий 56-битный ключ, работающий с 64-битными блоками[3]. Это архетипический блочный шифр - алгоритм, который берет строку битов открытого текста фиксированной длины и преобразует ее в строку битов зашифрованного текста такой же длины. Дизайн DES позволяет пользователям реализовать его на оборудовании и использовать для однопользовательского шифрования, например файлов, хранящихся на жестком диске в зашифрованном виде.

Расширенный стандарт шифрования (AES).

Это спецификация Национального института стандартов и технологий (NIST) для шифрования электронных данных. Он также помогает зашифровать цифровую информацию, такую как телекоммуникационные, финансовые и правительственные данные. Используется правительственными агентствами США для конфиденциальных несекретных материалов[3]. AES состоит из алгоритма с симметричным ключом: и шифрование, и дешифрование выполняются с

использованием одного и того же ключа. Это итеративный блочный шифр, который работает путем многократного повторения определенных шагов. Он имеет размер блока 128 бит с размерами ключей 128, 192 и 256 бит для AES-128, AES-192 и AES-256 соответственно. Дизайн AES делает его использование эффективным как в программном, так и в аппаратном обеспечении, а также работает на нескольких сетевых уровнях.

Алгоритмы асимметричного шифрования (криптография с открытым ключом).

Этот класс алгоритмов шифрования был введен для решения проблем управления ключами[3]. Они включают в себя как открытый, так и закрытый ключ. Открытый ключ является общедоступным, а отправитель хранит секретный ключ в секрете. Асимметричное шифрование использует пару ключей, состоящую из открытого ключа, доступного для всех, и закрытого ключа, принадлежащего только владельцу ключа, что помогает обеспечить конфиденциальность, целостность, аутентификацию и невозможность отказа при управлении данными.

Алгоритм Rivest Shamir Adleman (RSA).

RSA — это криптосистема с открытым ключом для шифрования и аутентификации в Интернете. RSA использует модульную арифметику и теорию элементарных чисел для выполнения вычислений с использованием двух больших простых чисел. Система RSA широко используется в различных продуктах, платформах и отраслях. Это один из де-факто стандартов шифрования. Такие компании, как Microsoft, Apple и Novell, встраивают алгоритмы RSA в свои операционные системы[5]. RSA - самый популярный асимметричный алгоритм. Вычислительная сложность факторизации больших целых чисел, являющихся произведением двух больших простых чисел, лежит в основе безопасности

алгоритма RSA[3]. Умножение двух простых чисел легко, но RSA основан на сложности вычисления исходных чисел из произведения.

Криптография эллиптических кривых (ECC).

ECC — это современная криптография с открытым ключом, разработанная, чтобы избежать более широкого использования криптографических ключей. Асимметричная криптосистема зависит от теории чисел и математических эллиптических кривых (алгебраической структуры) для генерации короткого, быстрого и надежного криптографического ключа. Криптография с эллиптической кривой была предложена для замены алгоритма RSA из-за небольшого размера ключа ECC.

Методы криптографии, используемые некоторыми облачными гигантами.

Google принял несколько уровней шифрования для защиты данных на своей платформе Google Cloud. Google использует алгоритмы шифрования Advanced Encryption Standard (AES 128 и AES 256) для шифрования данных, хранящихся на своей облачной платформе. Google делит данные о клиентах на несколько частей и шифрует каждый фрагмент разными ключами шифрования[4]. Данные и сгенерированный ключ шифрования объединяются другим ключом шифрования, обеспечивающим еще один уровень защиты, и эти ключи шифрования используются исключительно в центральной службе управления ключами Google[4]. Когда часть данных обновляется, она шифруется новым ключом, а не старым ключом. Поскольку каждый фрагмент данных зашифрован специальным ключом, если один фрагмент данных будет взломан, это не повлияет на другие фрагменты. Google использует списки управления доступом (ACL), чтобы гарантировать, что каждый фрагмент может быть расшифрован только службами Google, имеющими полномочия доступа в данный момент[4]. Это обеспечивает защиту и

безопасность данных, предотвращая несанкционированный доступ. Глобальное распределение фрагментов данных означает, что для того, чтобы злоумышленник получил доступ к данным, он должен прежде всего найти все местоположения различных фрагментов, соответствующих нужным им данным, а также знать ключи шифрования каждого отдельного фрагмента этих данных. Amazon S3 (Simple Storage Service) хранит объекты с избыточностью на нескольких объектах в регионе Amazon S3 [6]. Эта избыточность помогает восстановить данные, если есть проблемы с повреждением данных. Кроме того, Amazon S3 также использует управление версиями для резервирования каждой версии каждого объекта, хранящегося в Amazon S3 [2]. Управление версиями позволяет легко восстанавливаться после непреднамеренных действий пользователя и сбоев приложений[6]. Шифрование на стороне сервера, используемое Amazon, когда данные находятся в состоянии покоя, т.е. хранятся на дисках в центрах обработки данных Amazon S3, аналогично шифрованию Google и использует 256-битный AES для шифрования данных[4]. Microsoft принимает на себя общую ответственность, когда дело доходит до обеспечения безопасности и конфиденциальности данных на их облачной платформе Azure[5].

В этой статье обсуждались различные криптографические алгоритмы, используемые в облачных вычислениях, и рассматривались некоторые из криптографических алгоритмов, используемых некоторыми крупными агентами в облачных вычислениях.

Использованные источники:

1. The NIST Definition of Cloud Computing [Электронный ресурс] // URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (дата обращения 10.06.2021).

2. Velte A.T. Cloud Computing: A Practical Approach / A.T. Velte, T.J. Velte, R. Elsenpeter. – New York: The McGraw-Hill Companies, Cop. 2010. – 334 c.
3. Stallings W. Cryptography and Network Security: Principles and Practice, 7th Edition / W. Stallings. – London: Pearson plc, Cop. 2017. – 766 c.
4. Encryption at rest in Google Cloud [Электронный ресурс] // URL: https://cloud.google.com/security/encryption/default-encryption/#encryption_of_data_at_rest (дата обращения 10.06.2021).
5. ISO/IEC 27001:2013 Information Security Management Standards [Электронный ресурс] // URL: https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001 (дата обращения 12.06.2021).
6. Janakiram MSV. Amazon Brings Artificial Intelligence To Cloud Storage To Protect Customer Data [Электронный ресурс] // URL: https://www.forbes.com/sites/janakirammsv/2017/08/20/amazon-brings-artificial-intelligence-to-cloud-storage-to-protect-customer-data/?sh=28d6d70d7432 (дата обращения 14.06.2021).