(19) Евразийское патентное ведомство

(21) 201650074 (13) A2

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2019.08.30

(22) Дата подачи заявки
2016.12.13

(51) Int. Cl. ***G06F 21/00*** (2013.01)

(54) ВЕРИФИКАЦИЯ ХРАНИМЫХ ДАННЫХ ЧЕРЕЗ ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ ХРАНЕНИЯ С ИСПОЛЬЗОВАНИЕМ РАСПРЕДЕЛЕННОЙ БАЗЫ ДАННЫХ С НЕИЗМЕНЯЕМЫМИ ОБЪЕКТАМИ

(96) **2016000115 (RU) 2016.12.13**

(71) Заявитель:
АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ "УНИВЕРСИТЕТ ИННОПОЛИС" (RU)

(72) Изобретатель:
Тормасов Александр Геннадьевич, Ибрагимов Максим Константинович, Крутиков Александр Александрович, Малышев Вадим Владимирович (RU)

(74) Представитель:
Липатов А.Н. (RU)

(57) Система и метод, в котором в договоре между потребителем сервиса и предоставляющим сервис хранения данных включено значение параметра верификации хранимых данных. В договоре указываются измеряемые, численные значения, являющиеся одним из уровней сервиса, предоставляемого верификатором. Верификатор отвечает за соответствие данных потребителя данным в сервисе хранения данных. Потребитель сервиса использует арм клиент, который перенаправляет и обрабатывает сервисные запросы потребителя на прокси. Арм клиент использует Агента безопасности, который отвечает за безопасное использование ключей потребителя сервиса. Прокси перенаправляет и обрабатывает запросы от арм клиента на сервис хранения данных, являющийся совокупностью хранилищ данных.

201650074 A2

201650074 A2

Описание изобретения

Верификация хранимых данных через определение параметров хранения с использованием распределенной базы данных с неизменяемыми объектами

G06F 21/00

Область изобретения

Настоящее изобретение относится к вычислительным системам и, в частности, к системам и методам для электронно-вычислительных машин, для соглашения об уровне предоставления услуги, для верификации хранимых данных через определение параметров хранения с использованием распределенной базы данных с неизменяемыми объектами.

Сведения о предшествующем уровне техники

Проблема целостности данных в хранилищах данных в том числе арендуемых, сторонних и других хранилищах актуальна, особенно на фоне большого объема хранимых данных и популярности облачных хранилищ данных, которые зачастую арендуются и территориально разбросаны по всему миру. Сохранение целостности информации в хранилищах очень важно, т.к. любая информация, находящаяся в хранилищах, имеет ценность. Таким образом, существующая проблема частично решается путем периодической верификации данных в хранилищах. Проблема частично решается путем:

- разбития данных на большие группы и верификация группами;
- сравнения полученных или созданных метаданных, ассоциируемых с данными;
- сравнения контрольных значений баз данных после обновления.

Данные методы имеют проблемы в виде возможного изменения данных до или после верификации, недостоверности переданных и полученных данных. Таким образом, существующая проблема верификации данных в хранилищах не решена.

Все эти проблемы требуют решения.

Сущность Изобретения

Соглашение об уровне предоставления услуги (англ. Service Level Agreement (SLA)) — термин методологии ITIL, обозначающий формальный договор между заказчиком (в рекомендациях ITIL заказчик и потребитель — разные понятия) услуги и

её поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги.

Заказчик **101** (Customer, потребитель сервиса) –– это покупатель товаров или услуг. Заказчик для поставщика IT-услуг — это человек (группа людей), который заключает соглашение с поставщиком на предоставление IT-услуг и отвечает за то, чтобы предоставленные услуги были оплачены, как показано на Фиг. 1.

Поставщик услуг (Service provider, предоставляющий сервис) — это организация, поставляющая услуги одному или нескольким внутренним или внешним заказчикам.

Потребитель сервиса (заказчик) может являться одним или более вариантами из списка:

- индивидуальный пользователь;
- коллективный пользователь;
- корпоративный пользователь.

Конфигурирование данного SLA может являться частью внешнего контракта при заключении договора потребителя сервиса с центром данных. Данный SLA задается потребителем сервиса при изменении, создании файлов или метаданных файлов.

Договор имеет значение параметра верификации, который определяется заключаемым договором между потребителем сервиса и предоставляющим сервис хранения данных, в котором:

- указываются измеряемые, численные значения, являющиеся одним из уровней сервиса предоставляемым верификатором, который отвечает за соответствие данным потребителя с данными в сервисе хранения данных;
- параметр верификации соответствует выполнению одного или более условий предоставляемого сервиса из списка:
    - действий;
    - места;
    - времени;
    - результата исполнения.

АРМ Клиент 102 (Клиентское ПО, Client Software) — приложение, размещенное на компьютере потребителя сервиса. АРМ Клиент может перехватывать запросы Пользовательского приложения и обеспечивает корректное взаимодействие с Прокси, как показано на Фиг. 1.

Система для реализации изобретения включает в себя вычислительное устройство общего назначения в виде компьютера или компьютерной системы. Компьютер – устройство или система, способная выполнять заданную четко

определенную измеряемую последовательность операций. Компьютерная система — любое устройство или группа взаимосвязанных, или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных. Компьютерная система может иметь один или более классов назначения: настольный, интернет устройство, суперкомпьютеры, малые и мобильные устройства и другие возможные варианты.

Прокси 103 (Proxy) — приложение, размещенное на выделенном сервере в локальной сети предприятия. Прокси принимает запросы от АРМ Клиента и обеспечивает корректное взаимодействие с сервисом хранения данных. Прокси также отвечает за взаимодействие с распределенной базой данных с неизменяемыми объектами, как показано на Фиг. 1.

Сеть блокчейн – распределенная база данных с неизменяемыми объектами 104. Таким образом, сеть блокчейн может также являться распределённой базой данных, которая содержит увеличивающийся список записей, называемыми блоками и выстроенной по определенным правилам, защищенных от фальсификации и изменения. Т.е. сеть блокчейн может иметь выстроенную по правилам, согласно технологии Blockchain, цепочки из формируемых блоков транзакций, иметь API (прикладной интерфейс пользователя) и служит хранилищем немодифицируемых данных, как показано на Фиг. 1.

Распределенной базой данных с неизменяемыми объектами могут являться Bitcoin, Ethereum, Litecoin, Blackcoin, Dash, Namecoin, Bytecoin, BOLOS, Eris, Lisk, NEM, GEO, CoinJoin, Lightning Network, Bolt, Ripple.

Сервис хранения данных 105 — сервис, предоставляющий услуги хранения данных, как показано на Фиг. 1.

Сервис хранения данных может являться как объектным хранилищем, так и блочным хранилищем.

Блочные хранилища (иногда называемые хранилищами томов) выставляют для пользователя блочные устройства. Пользователи взаимодействуют с блочными хранилищами путем присоединения томов к своим работающим экземплярам.

Объектное хранилище — хранилище, доступ к которому осуществляется через REST API и которое хранит произвольные бинарные объекты, доступ к которым так же предоставляется, например, с помощью REST, RESTLESS API и другими.

Метаданные пишутся Прокси, отдельными файлами и шифруются собственным ключом, к которому АРМ Клиент доступа не имеет. В свою очередь, данные потребителя

сервиса шифруются, расшифровываются только на АРМ Клиенте, собственными ключами, к которым Прокси доступа не имеет.

Мы считаем, что все данные подвергнуты контролю целостности, например, сигнатурой или любыми другими способами.

Данные и метаданные могут хранится в зашифрованном виде. Хеш считается от зашифрованных данных и публично доступен. Хеш может возвращаться как часть процедуры транзакции на АРМ Клиент.

Часть алгоритма верификации может использовать методы проверки целостности (например Хеш), восстановления данных, электронную цифровую подпись, гомоморфное шифрование, квантовое шифрование и другие методы. Данными алгоритмами могут быть: MD5, SHA-1, SHA-2, ГОСТ Р 34.11, TTH, ED2K, AICH, CRC-32, HMAC, FDH, схема Эль-Гамаля, DSA, ECDSA, ГОСТ Р 34.10-2012, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.310-2004, схема Шнорра, схема BLS, схема GMR, RSA, PKCS#1, RSA-PSS, ECC, n,k-схема и другие. Под подписью, мы понимаем, полученный в результате криптографического (шифровального) преобразования информации с использованием закрытого ключа подписи данные предназначенные для защиты данных от подделки, а также от внесения несанкционированных изменений, возможны другие реализации. Данные методы могут быть совмещены друг с другом, в том числе с проверкой целостности восстанавливаемых данных.

Приведенные ниже утверждения о работе системы. методов и окружения относятся к конкретным вариантам реализации изобретения. В случае их нарушения в какой-либо реализации применимость описания изобретения не ограничивается, так как сделанные ниже предположения об условиях, окружении, системы и методов не являются безусловными требованиями к изобретению, а являются одним из возможных вариантов, не влияющим на суть предложенных методов и системы.

Мы считаем, что сервис хранения данных и сети связи от Прокси до сервиса хранения данных считаются одним целым. Вопрос коммуникации, надежности каналов связи не рассматриваются как часть данной системы.

Мы считаем, что алгоритмы шифрования считаются неломаемыми. Алгоритмы шифрования считаются не сломанными и не взломанными. Случай взлома алгоритмов шифрования не рассматривается как часть данной системы.

Мы считаем, что аутентификация потребителя сервиса на АРМ Клиенте считается неломаемой и корректной. Случай взлома аутентификации не рассматривается как часть

данной системы. Ключи шифрования потребителя сервиса уникальны, известны только ему и безусловно защищены ими.

1. **SLA по верификации**

Мы считаем, что АРМ Клиент считается доверенным субъектом. Вопрос коммуникации, надежности каналов связи не рассматриваются как часть данной системы.

Мы считаем, что распределенная база данных с неизменяемыми объектами является доверенной и неломаемой, т.е. алгоритмы, используемые в распределенной базе данных невозможно взломать с помощью Bruteforce или другими известными способами. Данные полученные от распределенной базы данных с неизменяемыми объектами – корректны, что включает в себя полную безопасность коммуникаций.

Данный SLA задаётся потребителем сервиса при создании файлов и постоянно используется в дальнейшем при изменении файла или метаданных файла.

АРМ Клиент непосредственно не взаимодействует с распределенной базой данных с неизменяемыми объектами.

Сборщик транзакций 201 – сущность, которая формирует транзакции для записи в распределенную базу данных с неизменяемыми объектами. Код Сборщика транзакций может выполняться как в Прокси, как показано на Фиг. 2а, так и в АРМ Клиенте, как показано на Фиг. 2б, но не являться их частью.

В одной из реализации изобретения транзакцию начинает формировать АРМ Клиент, передает частично данные на Прокси. Прокси заканчивает формирование транзакции, отправляет в Сервис хранения данных и одновременно отправляет верифицирующую информацию в распределенную базу данных с неизменяемыми объектами.

Cloud – идентификатор сервиса хранения данных. FID – ID файла или другие методики определения файла. Bucket – логический элемент хранилища, контейнер для сохраненных объектов или другие методики хранения объектов. Version – версия файла. Хеш – Хеш изменений к файлу, или Хеш полностью файла, который может строить как Merkle Tree подХешей для отдельных сегментов файла или могут применяться другие методы Хеширования и восстановления.

Предложение: SLA может определяться тем, что отрицательный ответ должен приходить не чаще чем n раз в год. Если положительный ответ не пришёл за некоторый тайм-аут, то ответ считается отрицательным.

При верификации с использованием распределенной базы данных с неизменяемыми объектами в любой момент времени после этого можно проверить утверждение о том, что данный файл был записан. Данные для верификации файла могут быть взяты от API сервиса хранения данных, из логов или каким-то другим способом. При верификации необходимо обеспечить возможность получения информации о содержимом транзакции: хеши данных, подписи АРМ Клиента и, если используется, подписи Прокси или другая информация, используемая в транзакции. Для верификации требуется получить данные транзакции и сверить их с восстановленными данными на сервисе хранения данных.

В одной из реализации изобретения различается 2 уровня SLA по верификации с использованием распределенной базы данных с неизменяемыми объектами, варианты реализации изобретения могут быть и другими:

1. Распределенная база данных с неизменяемыми объектами не задействована. Верификация не выполняется.
2. Верификация путем записи транзакции в распределенную базу данных с неизменяемыми объектами с подписью транзакции АРМ Клиентом и Прокси как показано на Фиг. 3. Ответом является однобитовый ответ: «да», «нет».

   1) АРМ Клиент отправляет через Прокси в сервис хранения данных заказ на модификацию или создание файла 305.

   2) АРМ Клиент получается информацию (FID, Cloud, Bucket, Version, Хеш) о заказе на модификацию или создание файла 310.

   3) АРМ Клиент формирует транзакцию А из FID, Cloud, Bucket, Version, Хеш (опционально), подписывает транзакцию А, состоящую из FID, Cloud, Bucket, Version, и отправляет транзакцию Прокси 315.

   4) (опционально) Прокси добавляет данные в транзакцию А от АРМ Клиента, подписывает их.

   5) Прокси отправляет транзакцию А в Сборщик транзакций 320, в котором транзакция А формируется и записывается в распределенную базу данных с неизменяемыми объектами 325.

   6) Прокси ждёт подтверждения блока с транзакцией А в распределенную базу данных с неизменяемыми объектами. Когда блок с транзакцией был подтверждён в распределенную базу данных с неизменяемыми объектами, то Прокси уведомляет АРМ Клиента о том, что верификация выполнена успешно 330.

2. **SLA типу распределенной базы данных с неизменяемыми объектами.**

Мы считаем, что распределенная база данных с неизменяемыми объектами является доверенной и неломаемой, т.е. алгоритмы, используемые в распределенной базе данных с неизменяемыми объектами невозможно взломать с помощью Bruteforce или другими известными способами. Данные полученные от распределенной базы данных с неизменяемыми объектами – корректны, что включает в себя полную безопасность коммуникаций.

Данный SLA задаётся потребителем сервиса. SLA определяется типом используемой распределенной базой данных с неизменяемыми объектами. Данный SLA комбинируется с пунктом 1.

В одной из реализаций изобретения различается 3 уровня SLA по распределенной базе данных с неизменяемыми объектами:

В одной из реализации изобретения распределенная база данных с неизменяемыми объектами может являться:

- публичной, которая доступна всем, каждый имеет права на чтение и добавление данных;
- ограниченной, в которой права на добавление данных имеет либо ограниченный определенный круг лиц, либо доступны всем, а права чтения имеет либо ограниченный определенный круг лиц, либо доступны всем;
- приватной, в которой права добавления данных централизованы, а права чтения имеет либо ограниченный определенный круг лиц, либо доступны всем.

1. **Публичная** - распределенная база данных с неизменяемыми объектами. потребитель сервиса выбирает SLA с использованием Публичной распределенной базой данных с неизменяемыми объектами. АРМ Клиента уведомил Прокси о выбранном SLA. Инициатор записи в распределенной базе данных с неизменяемыми объектами, который может являться АРМ Клиентом, Прокси, сервером хранения данных, регистрируется в Публичной распределенной базе данных с неизменяемыми объектами.
2. **Ограниченная** - распределенная база данных с неизменяемыми объектами. потребитель сервиса выбирает SLA с использованием Ограниченной распределенной базой данных с неизменяемыми объектами. АРМ Клиента

уведомил Прокси о выбранном SLA. Инициатор записи в распределенную базу данных с неизменяемыми объектами, который может являться АРМ Клиентом, Прокси, Сервисом хранения данных, регистрируется в Ограниченной распределенной базе данных с неизменяемыми объектами.

3. **Приватная** - распределенная база данных с неизменяемыми объектами. Потребитель сервиса выбирает SLA с использованием Приватной распределенной базой данных с неизменяемыми объектами. АРМ Клиента уведомил Прокси о выбранном SLA. Инициатор записи в распределенную базу данных с неизменяемыми объектами, который может являться АРМ Клиентом, Прокси, Сервисом хранения данных, регистрируется в Приватной распределенной базе данных с неизменяемыми объектами.

Варианты реализации изобретения могут быть другими.

3. SLA по Исполнителю верификации.

Данный SLA описывает исполнителя верификации. 401

В одной из вариантов реализации изобретения различается 4 уровня SLA по Исполнителю верификации:

1. Исполнителем верификации 401A является АРМ Клиент, как показано на Фиг.4а.
2. Исполнителем верификации 401B является Прокси, как показано на Фиг.4б.
3. Исполнителем верификации 401C является Сервис хранения данных, как показано на Фиг.4в.
4. Исполнителем верификации 401D является распределенная база данных с неизменяемыми объектами, как показано на Фиг.4г.

Варианты реализации изобретения могут быть другими.

4. Агент безопасности

Агент безопасности (АБ) – программа, отвечающая за безопасное использование ключей потребителя сервиса (PubU=AccessKey, PrivU, SecretKey) АРМ Клиентом. **108**

В одном из вариантов реализации изобретения АРМ Клиент взаимодействует с Агентом безопасности при выполнении следующих задач:

1. Проверить права (GET ACL);
2. Поделиться правами (PUT ACL);
3. Проверить подпись (CheckS3Sign).

При запуске Агента Безопасности программа выводит окно авторизации, предлагающее потребителю сервиса зарегистрироваться (Registrate) или аутентифицироваться (Authenticate).

После аутентификации АБ периодически подключается к АРМ Клиенту, запрашивая задачи на выполнение (Get Tasks). В случае если задачи имеются, АРМ Клиент передает их Агенту безопасности.

Варианты реализации изобретения могут быть другими, более стандартными в существующее время.

4.1. Регистрация в Агенте безопасности

Регистрация в Агенте безопасности – процесс сохранения ключей потребителя сервиса в шифрованном виде на компьютере потребителя сервиса или на другом носителе.

Регистрация в Агенте безопасности в одном из вариантов реализации изобретения происходит следующим образом, как показано на Фиг. 5:

1. К моменту регистрации потребитель сервиса либо уже имеет ключи на руках, либо получает ключи (GenKeys). 505
2. Потребитель сервиса добавляет ключи потребителя сервиса в пользовательскую папку или другое место хранения ключей (PutKeys). 510
3. Потребитель сервиса запускает АБ и выбирает команду «Зарегистрироваться». Потребитель сервиса придумывает пароль Password. 515
4. АБ зашифровывает хранящиеся ключи потребителя сервиса, используя пароль Password, как ключ шифрования. 520
5. АБ формирует хэш от пароля Password (MakeHash). 525
6. АБ сохраняет зашифрованные ключи потребителя сервиса и хэш от пароля (EncryptUserKeys). 530

Варианты реализации изобретения могут быть другими.

4.2. Аутентификация в Агенте безопасности

Аутентификация в Агенте безопасности – процесс подтверждения потребителем сервиса знания пароля Password.

Аутентификация в АБ в одном из вариантов реализации изобретения может происходить следующим образом, как показано на Фиг. 6:

1. Потребитель сервиса вводит пароль Password. 605
2. АБ вычисляет хэш от пароля и сверяет его с хранящимся хэшем. 610
3. Проверка совпадения хешей. 615
   3.1. Если аутентификация пройдена успешно, потребитель сервиса аутентифицирован 620, АБ расшифровывает ключи потребителя сервиса, используя в качестве ключа расшифрования – пароль Password. Расшифрованные ключи АБ сохраняет в оперативной памяти. 625
   3.2. Если нет, то выходит оповещение об отказе в доступе. 630

Варианты реализации изобретения могут быть другими.

4.3. Защищенное использование ключей потребителя сервиса

После успешной аутентификации Агент безопасности начинает периодически запрашивать у АРМ Клиента задачи на обработку.

АРМ Клиент отправляет Агенту безопасности накопившиеся задачи, если таковые имеются.

АБ в одном из вариантов реализации изобретения выполняет 3 функции:

1. Расшифровка записи списка контроля доступа (AclRow) и передача файловых ключей АРМ Клиенту (задача проверки GET ACL), как показано на Фиг. 7:
   1.1. АБ проверяет подпись (CheckSign) полученных данных от АРМ Клиента. 705
   1.2. АБ формирует ключ расшифровки записи списка контроля доступа (AclRow). 710
   1.3. АБ расшифровывает запись списка контроля доступа (AclRow). 715
   1.4. АБ передает содержимое записи списка контроля доступа. 720
2. Зашифровать файловые ключи, сформировать запись списка контроля доступа (AclRow) и передать ее АРМ Клиенту (задача передачи прав PUT ACL), как показано на Фиг. 8:
   2.1. АБ формирует ключ шифрования записи списка контроля доступа (AclRow). 805
   2.2. АБ шифрует содержимое записи списка контроля доступа (AclRow). 810

2.3.АБ формирует запись списка контроля доступа (AclRow). 815

2.4.АБ подписывает запись списка контроля доступа (AclRow). 820

3. Проверить корректность S3-подписи (задача CheckS3Sign), как показано на Фиг. 9:

3.1.АБ проверяет подпись S3-запроса (CheckS3Sign), полученную от АРМ Клиента. 905

Варианты реализации изобретения могут быть другими.

4.4. Экспорт Ключей

Экспорт ключей в Агенте безопасности – процесс передачи ключей потребителя сервиса в хранилище.

Хранилище может являться пользовательским, сторонним, внутренним или каким-либо другим.

Экспорт ключей в АБ в одном из вариантов реализации изобретения, как показано на Фиг. 10, может происходить следующим образом:

1. Потребитель сервиса запрашивает ключи потребителя сервиса, введя пароль Password и указывая путь для сохранения path (ExportKeys). 1005
2. АБ расшифровывает ключи потребителя сервиса, используя пароль Password, введенный потребителем сервиса, как ключ расшифровки 1010, и сохраняет их в указанном пути для сохранения path (DecryptUserKeys) 1015.

Варианты реализации изобретения могут быть другими.

Краткое описание графических материалов

Приложенные графические материалы, которые используются для улучшения понимания изобретения, является частью настоящего описания, иллюстрирующие варианты реализации настоящего изобретения, совместно с текстовым описанием, служащее цели разъяснения настоящего изобретения.

На чертежах:

Фиг. 1. Иллюстрирует систему верификации хранимых данных;

Фиг. 2а. Иллюстрирует сборщик транзакций в Прокси;

Фиг. 2б. Иллюстрирует сборщик транзакций в АРМ Клиент;

Фиг. 3. Иллюстрирует сборщик транзакций в АРМ Клиент;

Фиг. 4а. Иллюстрирует исполнитель верификации – АРМ Клиент;

Фиг. 4б. Иллюстрирует исполнитель верификации – Прокси;

Фиг. 4в. Иллюстрирует исполнитель верификации – Сервис хранения данных;

Фиг. 4г. Иллюстрирует исполнитель верификации – распределенная база данных с неизменяемыми объектами;

Фиг. 5. Иллюстрирует регистрацию в Агенте безопасности;

Фиг. 6. Иллюстрирует аутентификацию в Агенте безопасности;

Фиг. 7. Иллюстрирует расшифровку записи и передача ключей;

Фиг. 8. Иллюстрирует шифровку ключей, формирование записи;

Фиг. 9. Иллюстрирует проверку подписи;

Фиг. 10. Иллюстрирует экспорт ключей.

Примечание

Изобретение разработано в рамках исполнения работ по государственному соглашению о предоставлении субсидии от 03.10.14 № 14.612.21.0001. Заказчик работ: Минобрнауки России.

Формула изобретения

Верификация хранимых данных через определение параметров хранения с использованием распределенной базы данных с неизменяемыми объектами

1. Метод, в котором в договоре между потребителем сервиса и предоставляющим сервис хранения данных включено значение параметра верификации хранимых данных верификатором, где:
    - указываются измеряемые, численные значения, являющиеся одним из уровней сервиса предоставляемым верификатором, который отвечает за соответствие данным потребителя с данными в сервисе хранения данных;
    - потребитель сервиса использует арм клиент, который обрабатывает сервисные запросы и перенаправляет потребителя на прокси;
        - где, прокси перенаправляет и обрабатывает запросы от арм клиента на сервис хранения данных, являющийся совокупностью хранилищ данных;
    - параметр верификации соответствует выполнению одного или более условий предоставляемого сервиса из:
        - действий;
        - места;
        - времени;
        - результата исполнения.
2. Метод по п. 1, в котором потребитель сервиса может являться одним или более вариантами из:

- индивидуальный пользователь;
- коллективный пользователь;
- корпоративный пользователь.

3. Метод по п. 1, в котором данными могут являться файлы и/или метаданные файла.
4. Метод по п. 1, где сервис хранения данных может являться объектным хранилищем и/или блочным хранилищем.
5. Метод по п. 1, по которому договор между потребителем сервиса и предоставляющим сервис имеет значение параметра верификации с использованием распределенной базы данных с неизменяемыми объектами.
6. Метод по п. 5, по которому параметр верификации с использованием распределенной базы данных с неизменяемыми объектами принимает значение, что верификация выполняется либо верификация не выполняется.
7. Метод по п. 1, где АРМ Клиент использует Агента безопасности, который отвечает за безопасное использование ключей потребителя сервиса.
8. Метод по п. 7, где Агент безопасности осуществляет один или более действий из:
   - сохранение ключей шифрования;
   - аутентификацию потребителя сервиса;
   - шифрование данных;
   - расшифрование данных;
   - формирование электронной цифровой подписи;
   - проверка электронной цифровой подписи;
   - экспорт ключей шифрования на стороннее хранилище.
9. Метод по п. 6, где параметр верификации данных обозначает верификацию данных путем записи информации о транзакции в

распределенную базу данных с неизменяемыми объектами с подписями транзакции осуществляемыми одним или более из:

- АРМ Клиентом;
- Прокси;

где в момент верификации осуществляется сравнение данных из транзакции с информацией относительно отправленных данных.

10. Метод по п. 9, где АРМ Клиент подписывает транзакции об отправке файла, а прокси подписывает транзакции об отправке метаданных файла.

11. Метод по п. 9, где как часть алгоритма верификация данных используется один или более методы из:

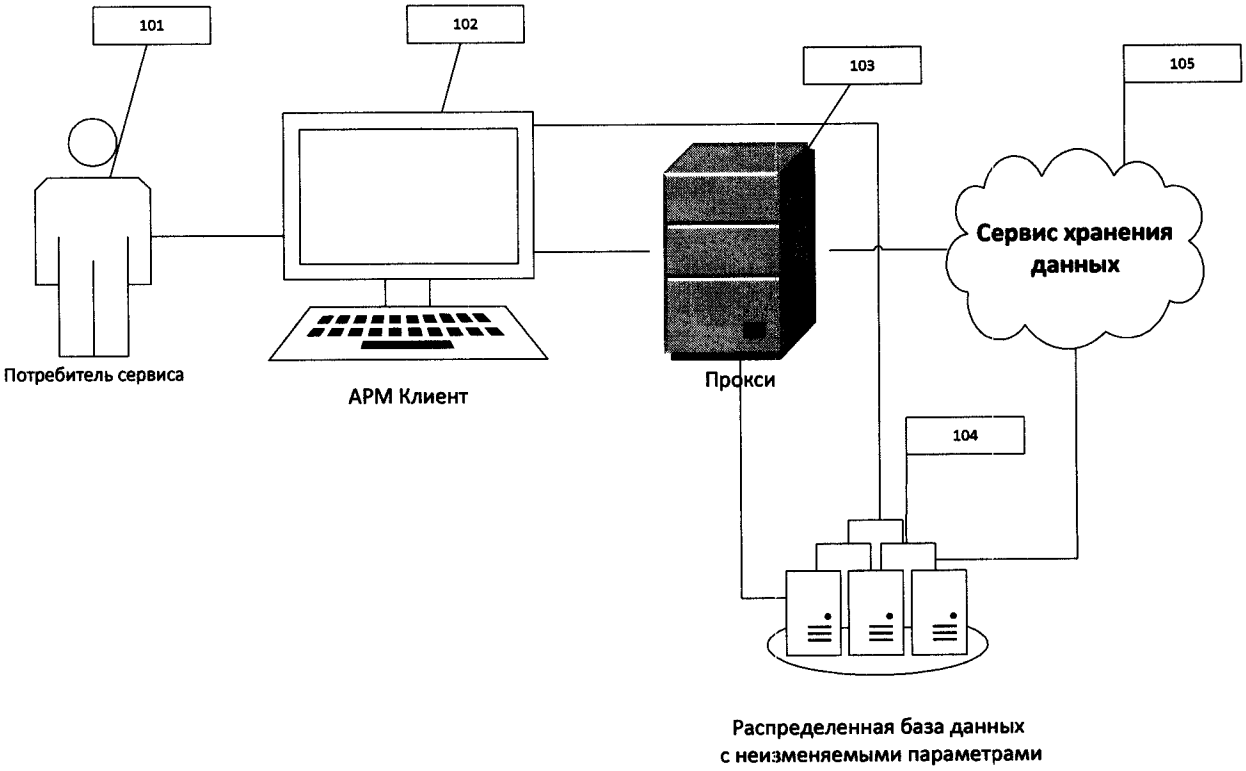
- проверка целостности;
- восстановление данных;
- электронная цифровая подпись;

12. Метод по п. 11, в котором используемые алгоритмы могут быть: MD5, SHA-1, SHA-2, ГОСТ Р 34.11, TTH, ED2K, AICH, CRC-32, HMAC, FDH, схема Эль-Гамаля, DSA, ECDSA, ГОСТ Р 34.10-2012, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.310-2004, схема Шнорра, схема BLS, схема GMR, RSA, PKCS#1, RSA-PSS ECC, n,k-схема.

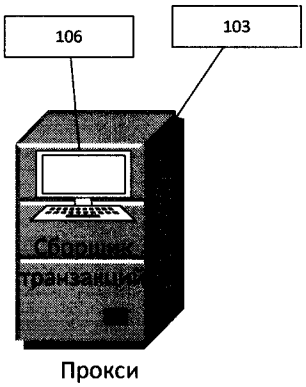
13. Метод по п. 6, где распределенной базой данных с неизменяемыми объектами может являться сеть блокчейн, которая:

- выстроена по правилам, согласно технологии Blockchain, цепочка из формируемых блоков транзакций;
- имеет API (прикладной интерфейс пользователя);
- служит хранилищем немодифицируемых данных.

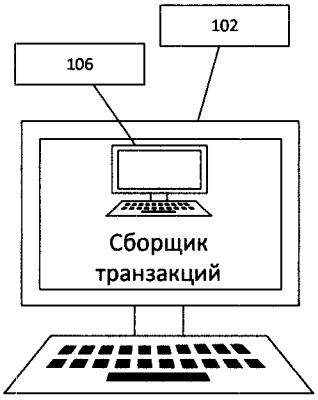
14. Метод по п. 13, в котором распределенной базой данных с неизменяемыми объектами может являться Bitcoin, Ethereum, Litecoin, Blackcoin, Dash, Namecoin, Bytecoin, BOLOS, Eris, Lisk, NEM, GEO, CoinJoin, Lightning Network, Bolt, Ripple.
15. Метод по п. 14, в котором распределенная база данных с неизменяемыми объектами может являться:
    - публичной, которая доступна всем, каждый имеет права на чтение и добавление данных;
    - ограниченной, в которой права на добавление данных имеет либо ограниченный определенный круг лиц, либо доступны всем, а права чтения имеет либо ограниченный определенный круг лиц, либо доступны всем;
    - приватной, в которой права добавления данных централизованы, а права чтения имеет либо ограниченный определенный круг лиц, либо доступны всем.


101
102
103
105
Потребитель сервиса
АРМ Клиент
Прокси
Сервис хранения данных
104
Распределенная база данных
с неизменяемыми параметрами

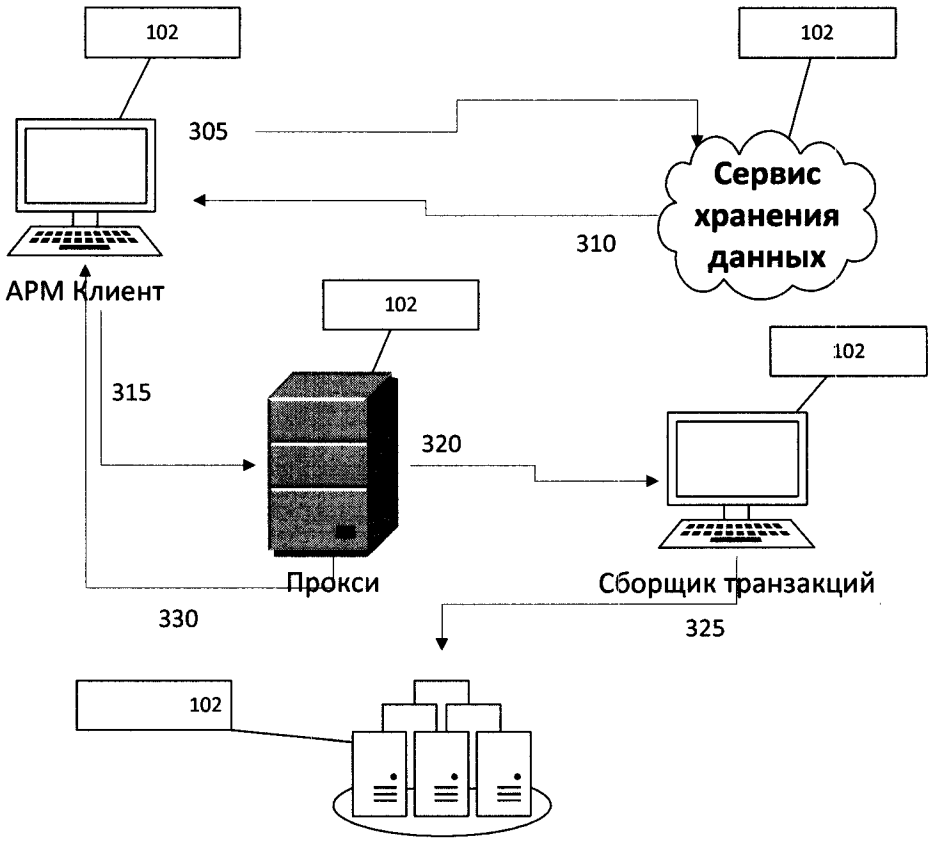
Фиг. 1



Фиг. 2а



Фиг. 2б

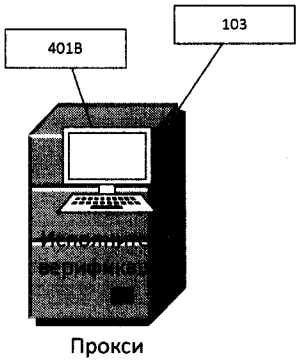


Распределенная база данных с неизменяемыми параметрами

Фиг. 3

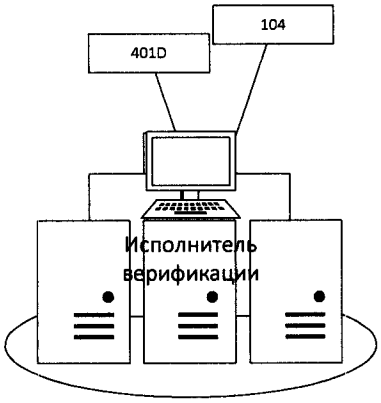

102
401A
Исполнитель
верификации
АРМ Клиент

Фиг. 4а


103
401B
Прокси

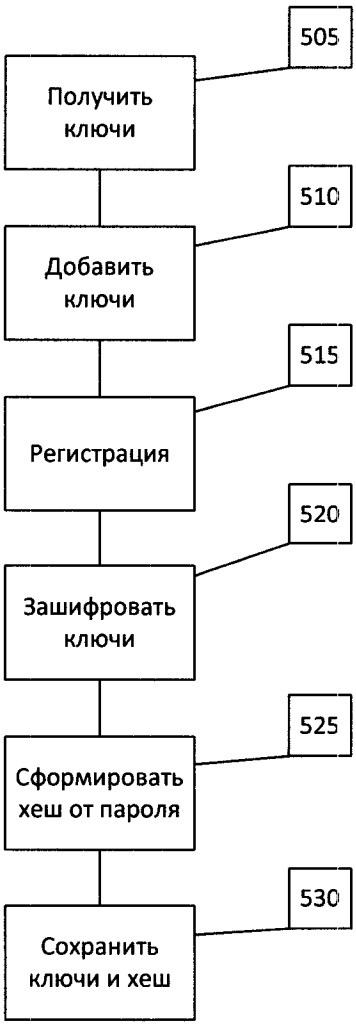
Фиг. 4б

Фиг. 4в

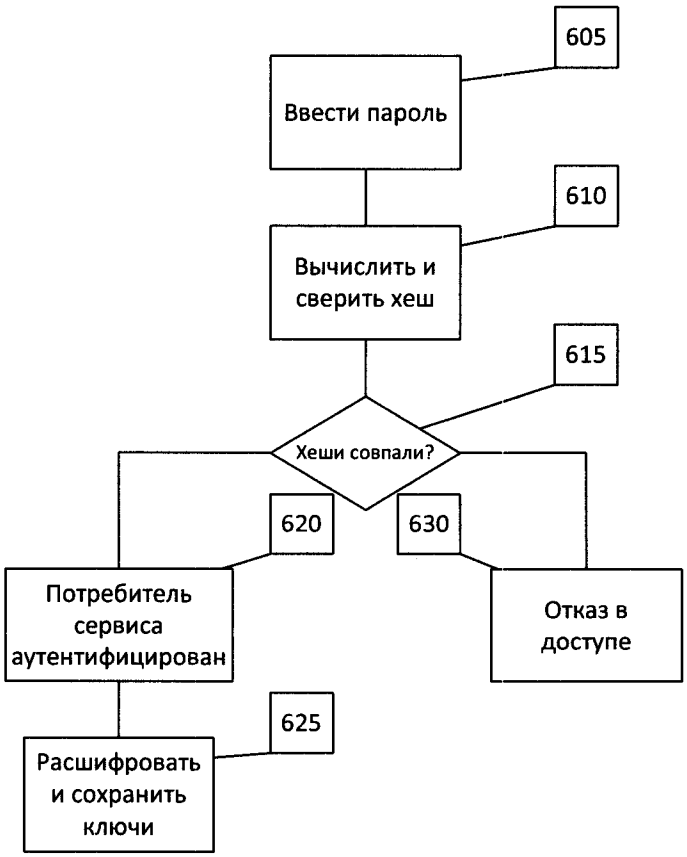


Распределенная база данных
с неизменяемыми параметрами

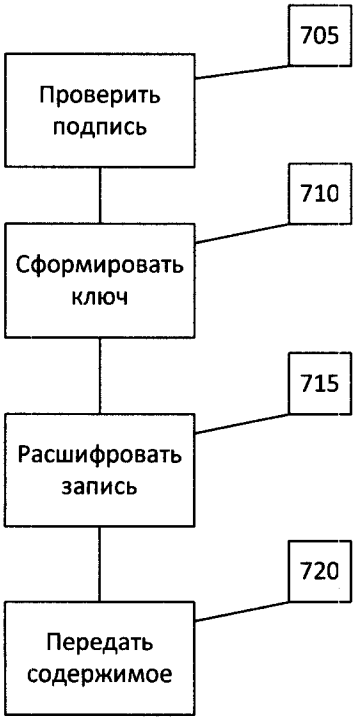
Фиг. 4г


505
Получить ключи
510
Добавить ключи
515
Регистрация
520
Зашифровать ключи
525
Сформировать хеш от пароля
530
Сохранить ключи и хеш

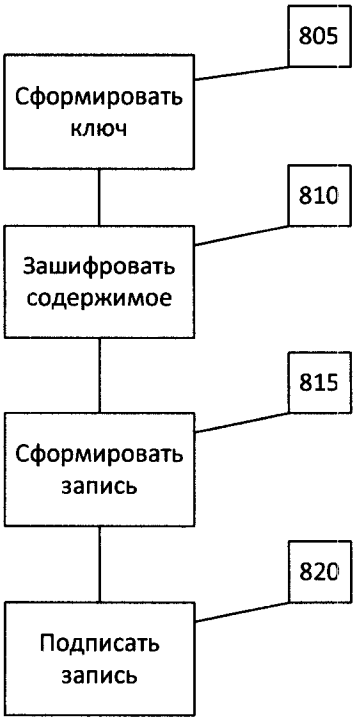
Фиг. 5


605
Ввести пароль
610
Вычислить и сверить хеш
615
Хеши совпали?
620
630
Потребитель сервиса аутентифицирован
Отказ в доступе
625
Расшифровать и сохранить ключи

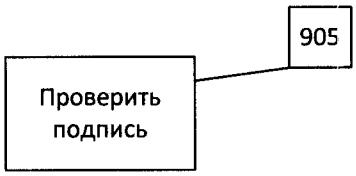
Фиг. 6


705
Проверить подпись
710
Сформировать ключ
715
Расшифровать запись
720
Передать содержимое

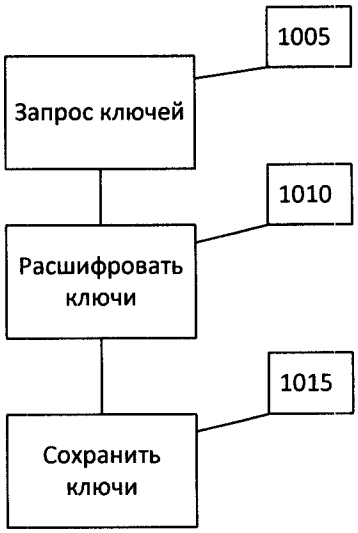
Фиг. 7


805
Сформировать ключ
810
Зашифровать содержимое
815
Сформировать запись
820
Подписать запись

Фиг. 8


905
Проверить подпись

Фиг. 9


1005
Запрос ключей
1010
Расшифровать ключи
1015
Сохранить ключи

Фиг. 10