УДК 00

Ситников Владислав Сергеевич

Студент

Научный руководитель: Барсук Игорь Вадимович

к.т.н., доцент

Ордена Трудового Красного Знамени федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технический университет связи и информатики»

БЛОКЧЕЙН СИТЕМЫ КАК БЕЗОПАСНОСТЬ УМНОГО ДОМА

Аннотация: Безопасность основных элементов умного дома – это одна из главных задач, которую нужно решить. Цифровизация и улучшение технологий приводит к тому, что люди все больше, и больше автоматизируют своё окружение, и получить информацию о владельце все легче.

Ключевые слова: Блокчейн, безопасность, дом, устройства, технологии

BLOCKCHAIN SYSTEMS AS SMART HOME SECURITY

Sitnikov Vladislav Sergeevich

Scientific adviser: Barsuk Igor Vadimovich

Abstract: The security of the main elements of a smart home is one of the main tasks that needs to be solved. Digitalization and technology improvement leads to the fact that people are automating their environment more and more, and it is becoming easier to get information about the owner.

Key words: Blockchain, security, home, devices, technology

Рассмотрение технологии Блокчейн для системы безопасности умного дома

В последнее время технология блокчейн используется в различных отраслях, включая финансы, дистрибуцию, здравоохранение и энергетику. Блокчейн был выбран в качестве одной из ключевых технологий, которые возглавят эпоху четвертой промышленной революции на Всемирном экономическом форуме 2016 года. Мировые институты рыночных исследований, Gartner и Deloitte также выбрали блокчейн в качестве одного из технологических трендов 2017 года . Блокчейн - хорошо известная технология распределенной бухгалтерской книги. Это может преодолеть ограничения косвенных и пассивных гарантий доверия, которыми обладают традиционные централизованные системы, и внедрить децентрализованную систему, которая может гарантировать пользователям прямые и активные доверительные отношения. Блокчейн может быть легко применен и интегрирован в различные отрасли, а целостность блока обеспечивает целостность данных. Блокчейн состоит из цифрового реестра, который записывает информацию о транзакциях, происходящих в сети, и распределяется между участниками сети. Копия Реестра распределяется между каждым участником сети. Когда происходит новая транзакция, она аутентифицируется с согласия всех участников. Блокчейн состоит из нескольких блоков, которые содержат определенную информацию о транзакции. Поскольку многочисленные блоки объединены в единую блокчейн-цепочку, произвольно изменять конкретные данные невозможно. Блоки соответствуют данным, хранящимся у большинства всех пользователей, где более 51% всех пользователей идентифицированы как подлинные блоки. Если данные какого-либо блока изменены или отсутствуют, их легко восстановить, поскольку в бухгалтерских книгах хранятся данные о хэш-значении. Практически невозможно изменить бухгалтерскую книгу на основе информации об одной

транзакции. Изменение данных требует одновременного взлома как минимум 51% всех блоков. Поскольку технология распределенной бухгалтерской книги открыта для всех участников сети, вся новая информация обновляется в режиме реального времени, и информации легко доверять и отслеживать. Устранение присутствия посредников на основе подхода распределенной одноранговой сети и без использования традиционных централизованных систем повышает эффективность и прозрачность транзакций. Это создает быструю и безопасную сетевую среду при меньших затратах. Основанный на сети P2P, блокчейн подключается к равному уровню всеми пользователями, действуя как сервер и одновременно как клиент. Это может решить проблему серверно-клиентской архитектуры, в которой несколько пользователей подключены и управляются через централизованный сервер в существующей сетевой системе.

Шлюз "Умный дом"

Ряд технологий для "умных домов" внедряется по мере роста интереса к жилой среде из-за технологического развития. "Умный дом" относится к жилой среде, оснащенной технологиями, которые могут автоматически управлять устройствами и системами. Управление этими средами зависит от множества переменных условий, таких как затраты, предпочтения жителей и типы зданий в зависимости от технологии. Сетевая структура, которая может автоматически регулировать температуру и уровни безопасности, а также эффективно взаимодействовать внутри и снаружи умных домов, может предоставить жителям широкий спектр условий жизни, повышая их удовлетворенность. Шлюз для разработки этих сетей обеспечивает функциональность для следующих концепций:

- Разнообразие домашних сетевых подключений.
- Домашняя сеть и интернет-соединения.
- Дистанционное управление и диагностика бытовой техники.

- Гибкие механизмы расширения и обновления программного обеспечения.
- Надежный и безопасный метод удаленного управления.

Реализация этих шлюзов направлена на создание устойчивого "умного дома", который может создавать дополнительную ценность при одновременном устранении различных уязвимостей существующих "умных домов".

Соображения безопасности шлюза "Умный дом"

Несколько устройств, в совокупности составляющих "умный дом", контролируются посредством обмена данными через шлюз. Такая конфигурация сети может раскрыть данные в доме, привести к нарушениям конфиденциальности, вызвать сбои в работе устройств и нанести вред пользователям. Когда пользователь получает доступ к сети "умный дом", реализованной в каждом домохозяйстве, данные, собранные устройствами в целевом формате, могут быть утечены. В отсутствие стандартов безопасности для умных домов и устройств возникают трудности с объединением различных разнородных устройств. По этой причине различные услуги не могут предоставляться пользователям бесперебойно. Безопасность шлюзов имеет важное значение, и ниже описаны требования безопасности к шлюзам в "умных домах".

- Конфиденциальность: Сети, настроенные в "умных домах", собирают и хранят множество данных, включая конфиденциальную информацию от жильцов. Доступ к этим данным должен быть доступен только уполномоченному персоналу и является важным элементом безопасности "умных домов". Для обеспечения конфиденциальности характеристик "умных домов" мы используем блокчейн с алгоритмом шифрования и настраиваем его с помощью ключа.
- Целостность: когда данные отправляются и принимаются между каждой конфигурацией, во время передачи данных не должно

происходить фальсификации. Хэш-функция снижает вероятность того, что эти данные будут фальсифицированы, и позволяет отслеживать и проверять, какие именно данные записаны.

- Аутентификация: функция аутентификации в конфигурациях сети "умный дом" предотвращает злоумышленные действия злоумышленника в обычной сети извне. Блокчейн используется для проверки того, что сеть является действительным участником, и может воспользоваться возможностью проверить это в определенное время, чтобы включить правильную конфигурацию сети "Умный дом".

Существующие исследования

Сивараман и др. исследовали и проанализировали уязвимости в системе безопасности сетевого уровня "умный дом" и предложили решения. Можно управлять сертифицированными устройствами и проверять их с помощью интернет-провайдера и управлять устройствами для умного дома даже во внешней интернет-среде. Однако этот подход неэффективен для обеспечения безопасности внутренней интернет-среды из-за нехватки пользовательских данных для анализа. Копос и др. проверили поток в доме и отсутствие конфиденциальных данных, используя Wireshark для таких устройств, как пожарные извещатели, при создании устройств для умного дома. Этот подход обеспечивает программные решения, но он не может быть совместим с другим программным обеспечением, кроме wireshark.

Ли и др. предложили обновление, которое управляет обновлениями встроенного программного обеспечения встроенных устройств с использованием блокчейна, аутентификацией с использованием цифровых подписей и применяет алгоритмы шифрования с использованием закрытых ключей. Этот механизм не обеспечивает решения для обеспечения безопасности небольшого умного дома, в котором небольшое количество встроенных устройств подключено друг к другу. Булл и др. предложили

шлюз, позволяющий централизованно управлять и настраивать с использованием SDN (программно-определяемая сеть) с учетом средств обеспечения гибкой и безопасной связи для быстро растущего числа устройств на базе Интернета вещей. Предлагаемый шлюз основан на централизованной методологии, что может привести к проблеме единой точки отказа. Инь и др. объединили схему защиты конфиденциальности с машинным обучением и предложили новый подход к безопасности, основанный на человекоцентричных вычислениях. Однако этот подход менее эффективен в случае отсутствия достаточного количества обучающих данных для создания модели машинного обучения. Панвар и др. обсудили различные угрозы безопасности и их решения в "умном доме". Они представили всесторонний обзор безопасности "умного дома" с точки зрения статистики различных атак. Пох и др. представил подход PrivHome, обеспечивающий конфиденциальность. Он обеспечивает аутентификацию, безопасное хранение данных и запросы для систем "умный дом". Он изучает и изменяет данные, передаваемые между пользователем, шлюзом, поставщиком услуг и устройством, для поддержки аутентификации данных и конфиденциальности. Шуран и др. представили влияние различных атак безопасности на "умный дом" и оценили их влияние как низкое, умеренное и высокое для соответствующих решений по их смягчению.

Другие подходы к обеспечению безопасности основаны на IoT и киберфизической системной безопасности, в которых используются различные новые технологии, такие как блокчейн, программно-определяемые сети и глубокое обучение.

Сеть шлюза "Умный дом" на основе блокчейна

Блокчейн, применяемый к шлюзам "умный дом", является важной частью аутентификации при передаче данных с сохранением целостности и конфиденциальности между устройствами и другими носителями. Хотя сеть "Умный дом" имеет централизованную сетевую форму в каждом умном доме, она была применена как централизованная к распределенной сети с использованием блокчейна на облачном уровне.

Шлюз "умный дом", основанный на предлагаемой блокчейне, имеет три уровня: уровень устройств, уровень шлюза и облачный уровень. Первый уровень, уровень устройств, состоит из датчиков и устройств, которые собирают и отслеживают данные в сетевой среде "умного дома" с помощью различных разнородных IoT, настроенных в "умном доме". Второй уровень, уровень шлюза, хранит данные, генерируемые уровнем устройств, и предоставляет их пользователям по мере необходимости. Третий уровень, облачный, регистрирует идентификатор шлюза и данные, обрабатываемые каждым шлюзом в блокчейне. Блоки являются общими, чтобы пользователи могли получать информацию в любое время и в любом месте. Это можно выразить так, как показано на рис. 1.

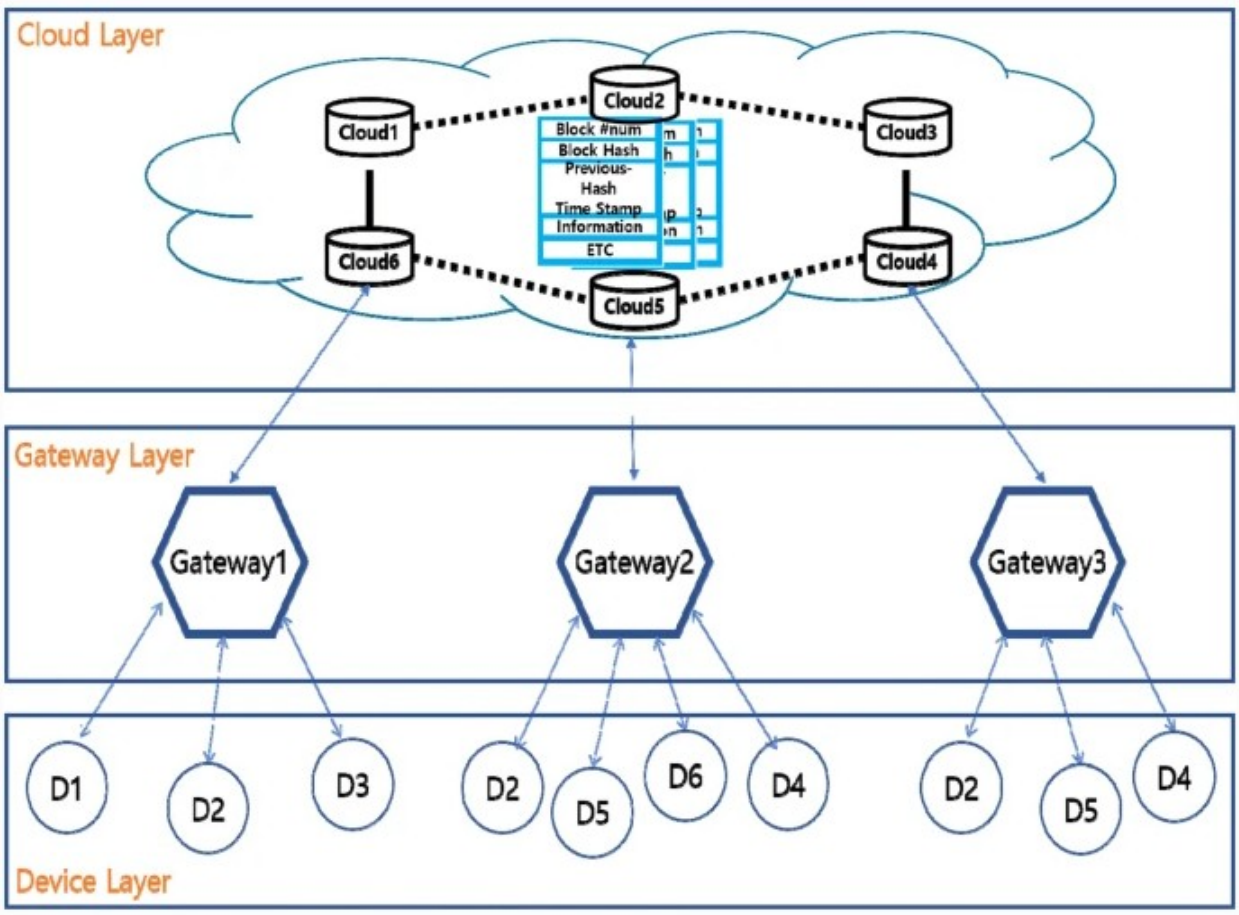

Рис. 1. Обзор конструкции предлагаемой сети

На рисунке 1 показана блок-схема предлагаемой архитектуры, которая позволяет собирать данные с конечных устройств, регистрировать их в блокчейне и представлять пользователям соответствующим образом. Для сбора и предоставления данных пользователю собранные данные подвергаются обработке и форматированию хэш-значений, создаются блоки и периодически проверяются для поддержания целостности, даже если происходит фальсификация данных. Анализ данных и поддержание качества должны проводиться постоянно, чтобы предоставлять пользователям только необходимую информацию.

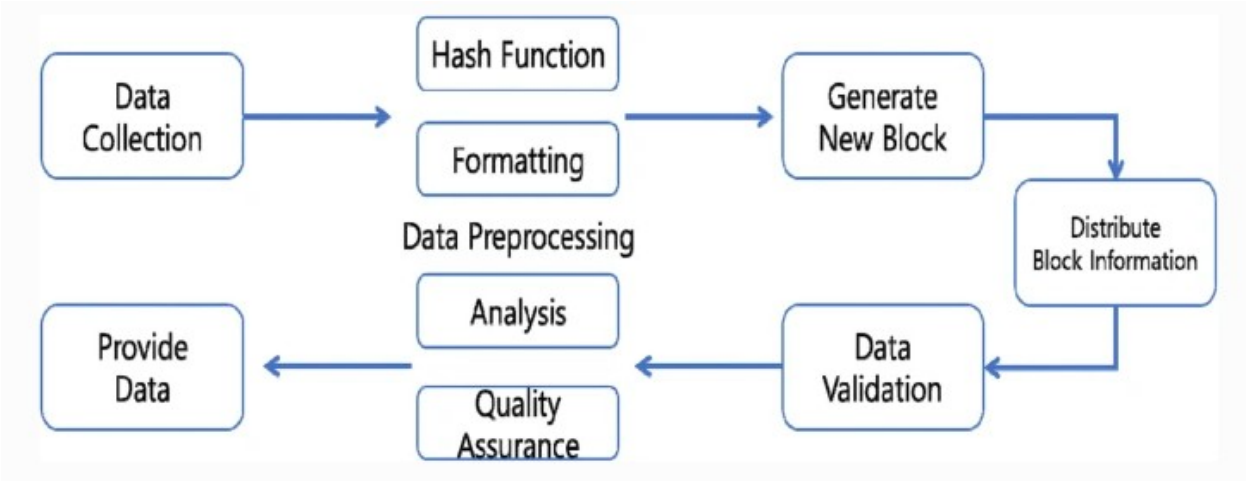

Рис. 2. Методологический поток облачной архитектуры для шлюза для умного дома на основе блокчейна

Устройства интернета вещей, настроенные в "умных домах", подключены к одному шлюзу, и каждому устройству присваивается идентификатор. Эти шлюзы и устройства имеют фиксированные идентификаторы и обладают вычислительной мощностью для работы алгоритмов шифрования и декодирования с помощью PKI и SHA2. Процессы сертификации, регистрации и хранения данных для процессов протокола взаимодействия устройства и шлюза, как показано на рис. 3.

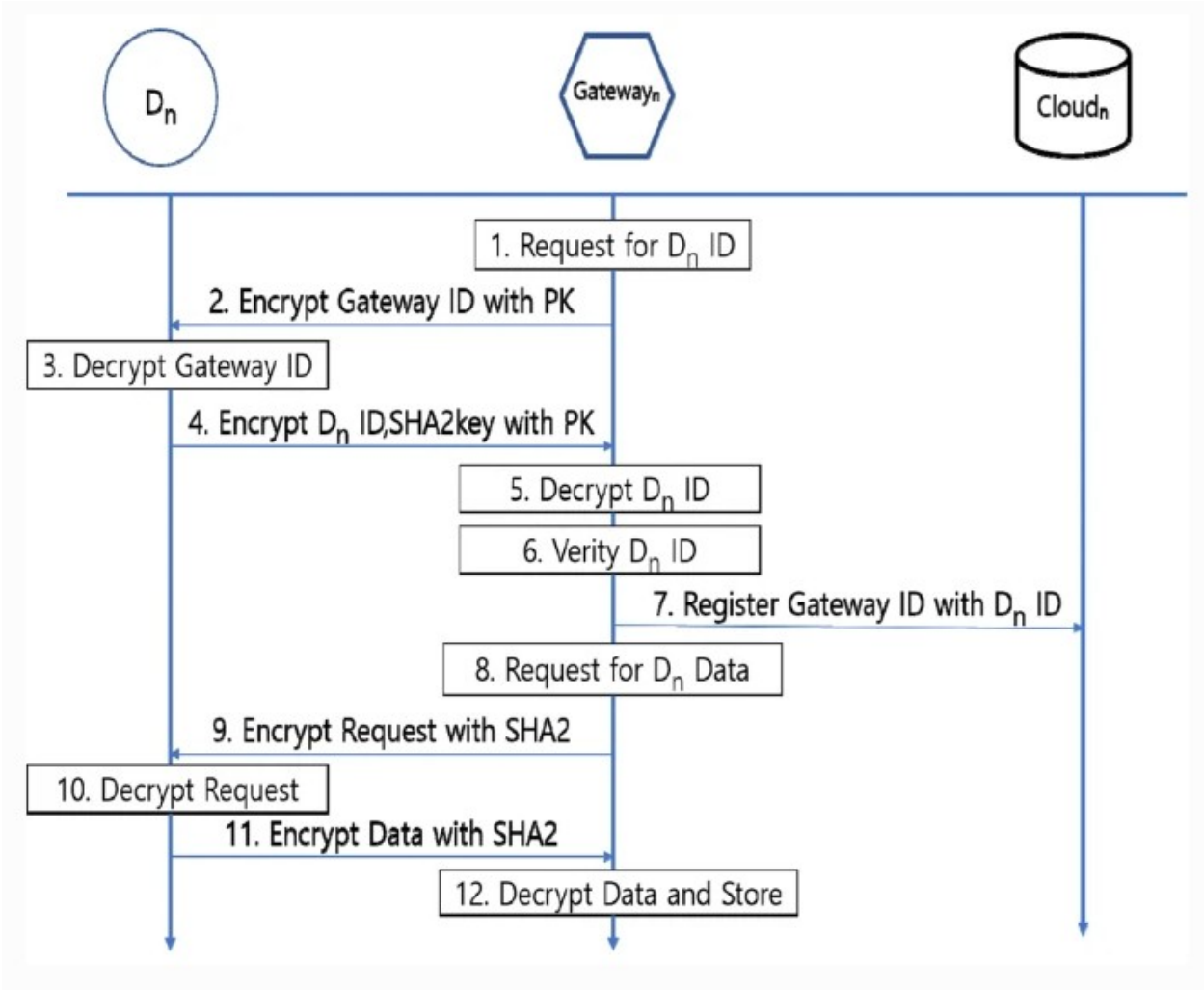

Рис. 3. Идентификация устройств и сбор данных

1. Устройства, сертифицированные для шлюза, всегда должны периодически проверяться. Dn на уровне устройств пытается зарегистрироваться напрямую или автоматически подключается к шлюзу. Шлюз запрашивает идентификатор у подключенного устройства или запрашивается для получения информации о подключенном устройстве.
2. Шлюз устройства реализует криптографический алгоритм для шифрования информации шлюза на устройстве и отправки сообщения. Устройства с помощью предварительно совместно используемых ключей декодируют зашифрованные сообщения.

3. Зашифрованные сообщения, содержащие информацию шлюза, расшифровываются и запрашиваются незарегистрированным или не за шифруемым шлюзом при их получении.
4. Чтобы поделиться ключом алгоритма шифрования SHA2 для непрерывной связи между устройствами и маршрутизатором, мы шифруем идентификатор устройства и ключ SHA2 для отправки сообщений на шлюз.
5. –6.Шлюз декодирует передаваемые сообщения, чтобы убедиться, что они зарегистрированы как обычные устройства.
7. После завершения процедуры идентификации между шлюзом и устройством мы сохраняем идентификатор устройства, зарегистрированный на шлюзе, в облаке. Шлюз со временем обменивается данными с облаком для обновления списка идентификаторов устройств.
8. Для сбора данных, генерируемых устройством, шлюз создает сообщение с запросом и отправляет его на устройство.
9. Сообщения о запросах данных шифруются с помощью ключа алгоритма паролей SHA2, который был проверен в предыдущем процессе.
10. –11.При передаче данных с помощью устройства запрашивается ключ к шлюзу декодирования зашифрованного сообщения и шифрования для передачи необработанных данных.
12. Шлюз сохраняет полученные необработанные данные путем их декодирования

Управление данными шлюза с использованием блокчейна

Сеть, состоящая из блокчейнов, гарантирует целостность процесса передачи данных и записей. Данные, сгенерированные конечными узлами, участвующими в сети, или сохраненные в базе данных, могут храниться с использованием алгоритма хэширования SHA-3 на основе необходимой сгенерированной информации. Эти блоки сравниваются в режиме реального времени в сети блокчейнов в облаке. Они проверяют данные, обнаруживая, существует ли подделанный блокчейн. Процесс регистрации и мониторинга данных шлюза на блокчейне можно представить на следующем рисунке. 4.

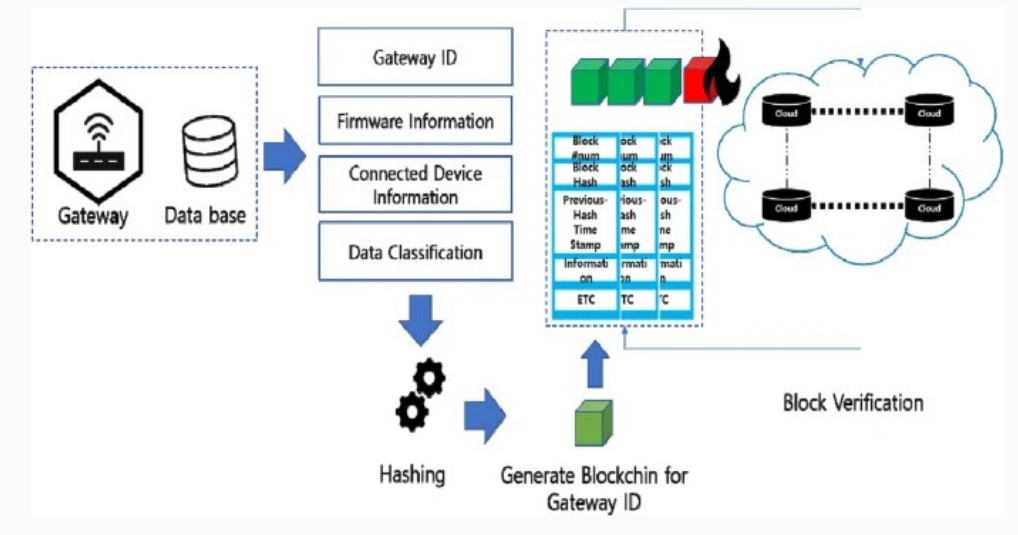

Рис. 4. Управление данными шлюза на основе блокчейна

Предварительная обработка данных внутри шлюза

Данные, генерируемые разнородными устройствами интернета вещей в "умном доме", передаются на шлюз "Умный дом", состоящий из различных размеров и типов данных. Шлюз "Умный дом" предлагаемой архитектуры должен точно управлять IoT и обрабатывать данные в соответствии с запросом пользователя. На рисунке 4 описывается процесс передачи данных из Интернета вещей в шлюз "Умный дом", где обработка данных разделена на три категории: сбор, предварительная обработка и хеширование.

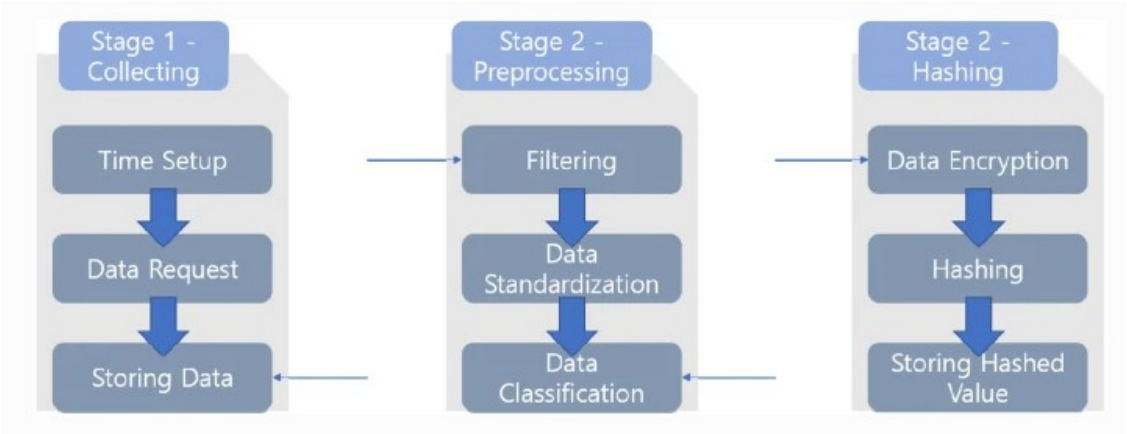

Рис. 5. Предварительная обработка данных шлюза

- Этап 1. Сбор: данные, сгенерированные устройством, передаются маршрутизатору в течение определенного времени. Когда на шлюзе требуются новые данные или когда происходит событие, данные запрашиваются у устройства. Затем необработанные данные отправляются и хранятся на устройстве, хранения данных в шлюзе.
- Этап 2. Предварительная обработка: необработанные данные, отправляемые с устройства, предварительно обрабатываются внутри шлюза. Для повышения эффективности использования пространства для хранения он фильтрует и сохраняет только те данные, которые необходимы маршрутизатору, на основе идентификатора устройства и хранятся с использованием процесса стандартизации и классификации.
- Этап 3. Хеширование: данные, генерируемые в "умном доме", содержат конфиденциальную информацию пользователя, поэтому ими можно управлять с помощью шифрования. Алгоритм SHA256 применяется на основе пароля, указанного пользователем, а общие данные устройства хранятся с помощью хэш-функции.

Использованные источники:

1. «Умный дом» [Электронный ресурс] — Режим доступа: \www/ URL: http://umnydom.kiev.ua/index.php?nma=catalog&fla=stat&cat_id=3&page=1&nums=24/ — 05.03.2011 г.

2. Перспективы рынка систем ”Умный дом” [Электронный ресурс] / Центр инженерных технологий CENTEC. — Режим доступа: \www/ URL: http://www. centecgroup.ru/press/articles/18/ — 02.03.2011 г. — Загл. С экрана.

3. Кузьмич А. Неутомимый труженик. Системы «Умного дома» [Текст]/ А. Кузьмич// Журн. S.M.A.R.T. — 2009. – № 2.- С. 10-13. 5. Категории «Умных домов» [Электронный ресурс] / Дом Бизнес Строй. — Режим доступа: \www/ URL: http://ruswires.net/post_1267720042.html/ — 04.03.2011 г. — Загл. С экрана.

4. IDC forecasts double-digit growth for smart home devices as consumers embrace home automation and ambient computing [Прогноз продаж умных «умный дом» устройств]. – IDC, 2021. – URL: https://www.idc.com/getdoc.jsp?containerId= prUS47567221 (accessed: 03.12.2021).

5. Fernandez E., Jung J., Prakash A. Security analysis of new intelligent home applications // Proceedings of the IEEE Symposium on Security and Privacy (SP). – San Jose, CA, 2016. – P. 636–654. – DOI: 10.1109/SP.2016.44.

6. Opening Pandora’s box: effective techniques for reverse engineering IoT devices / O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici, Y. Oren // Smart Card Research and Advanced Applications, CARDIS 2017. – Cham: Springer, 2018. – P. 1–21. – DOI: 10.1007/978-3-319-75208-2_1.

7. Полоцкий Р.Е. Что такое «умный дом»? // Алгоритм безопасности. – 2017. – № 4. – С. 4–7.

8. King N. Smart home – definition. – Intertek Research & Testing Centre, 2003. – URL: https://www.housinglin.org.uk/_assets/Resources/Housing/Housing_advice/Smart_Home_-_A_definition_September_2003.pdf (accessed: 03.12.2021).