АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ И УПРАВЛЕНИЕ ДАННЫМИ С ПОМОЩЬЮ БЛОКЧЕЙН-СИСТЕМЫ

А.Д. Эйнман, *Московский технический университет связи и информатики anastasia.859r65@gmail.com;*
И.А. Нагорный, *Московский технический университет связи и информатики, most2607@icloud.com.*

УДК 004.056.5:004.75

Аннотация. Развитие технологий привело к инновациям в оборудовании, а количество высокотехнологичных устройств растет с каждым днем. Эти устройства развертываются через интернет вещей. Устройства интернета вещей имеют ограничения, связанные с безопасностью как на программном, так и на аппаратном уровнях. Безопасные пользовательские интерфейсы позволяют преодолеть ограничения на уровне программного обеспечения, например, к интерфейсам внешнего пользователя легко получить доступ через общедоступные и частные сети. Интерфейсы подключаются к локализованному хранилищу для хранения данных, создаваемых устройствами интернета вещей. Локализованное хранилище, развернутое в закрытой среде, подключенное к устройствам интернета вещей, с точки зрения безопасности более эффективно, чем онлайн-серверы. Блокчейн появился как технология или метод, обладающий возможностями для обеспечения безопасной административной аутентификации и доступа к устройствам интернета вещей и их вычислительным данным децентрализованным способом с высокой надежностью и устойчивостью. В данной статье предлагаются методы аутентификации устройств, конечных пользователей и транзакций с использованием встроенных в блокчейн алгоритмов.

Ключевые слова: блокчейн; аутентификация; *IoT*; интернет вещей.

USER AUTHENTICATION AND DATA MANAGEMENT USING A BLOCKCHAIN SYSTEM

A.D. Einman, *Moscow Technical University of Communications and Informatics;*
I.A. Nagornyy, *Moscow Technical University of Communications and Informatics.*

Annotation. The development of technology has led to innovations in equipment, and the number of high-tech devices is growing every day. These devices are deployed via the Internet of Things. Internet of Things devices have security-related limitations at both the software and hardware levels. Secure user interfaces allow to overcome limitations at the software level, for example, external user interfaces can be easily accessed through public and private networks. The interfaces connect to a localized storage for storing data generated by IoT devices. Localized storage deployed in a closed environment, connected to Internet of Things devices, is more efficient from a security point of view than online servers. Blockchain has emerged as a technology or method with the capabilities to provide secure administrative authentication and access to Internet of Things devices and their computing data in a decentralized manner with high reliability and stability. This article suggests methods for authenticating devices, end users, and transactions using algorithms built into the blockchain.

Keywords: blockchain; authentication; *IoT*; Internet of things.

Введение

С быстрым ростом количества умных гаджетов и высокоскоростных сетей, которые используются для связи с этими умными устройствами, интернет вещей (*Internet of things, IoT*) за последние несколько лет привлек много внимания исследователей [1]. Эти встроенные устройства или устройства интернета вещей подключаются через общедоступные или частные сети, получают удаленный доступ и предоставляют желаемую функциональность. Публичные и частные сети используют сетевые протоколы для обмена информацией и взаимодействия между устройствами *IoT* [2].

Интернет вещей – это ресурсоемкие устройства, которые не способны защищать себя от вредоносных атак, таких как атака «человек посередине», *DOS*-атаки и т.д., и могут быть легко взломаны злоумышленниками. Для обеспечения безопасности важно внедрить надлежащие методы для пользователя, а также аутентификацию устройства и вычислительную транзакцию, чтобы убедиться, что устройства интернета вещей безопасны во всех отношениях [3]. Существует также потребность в системе для обеспечения взаимодействия между конечными пользователями и устройствами интернета вещей [4].

Многочисленные методы аутентификации [5] разработаны и развернуты для обеспечения безопасности устройств интернета вещей, но все они основаны на централизованной архитектуре и зависят от централизованного органа управления, такого как база данных или серверы системы. Центр управления проверяет конечных пользователей, системные устройства интернета вещей и записи связи между конечными пользователями и устройствами интернета вещей с использованием различных протоколов. Взаимная аутентификация, аутентификация на основе сертификатов и аутентификация на основе токенов – все это централизованные методы аутентификации. Эти методы имеют много недостатков, таких как высокие транзакционные вычислительные затраты, централизованные доверенные третьи стороны, единая точка отказа, отсутствие конфиденциальности и высокая вероятность взлома. Поскольку эти методы таким образом полагаются на доверенную третью сторону, возникают проблемы с двойной зависимостью [6]. На рис. 1 представлена проблема двойной зависимости. Владельцы системы могут отправлять одну и ту же транзакцию нескольким участникам системы.

Недостатком прямой аутентификации пользователей является то, что они аутентифицируют пользователей только с помощью имени пользователя или пароля. Таким образом, защищенность данного метода аутентификации довольно низкая.

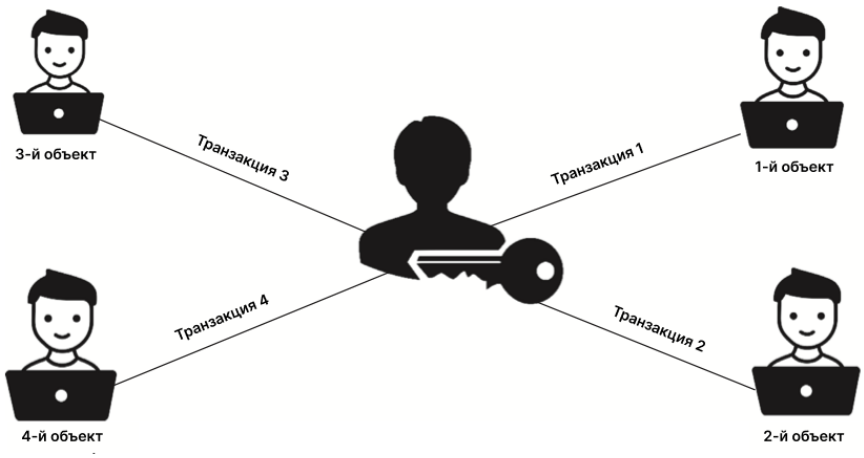

Рисунок 1

Метод открытой аутентификации для аутентификации пользователя – это централизованный метод, при котором все вычисления выполняются с использованием центрального идентификатора.

Метод групповой аутентификации разделяет метод аутентификации на нескольких узлах, но метод групповой аутентификации не использует значения хэш-ключа, поэтому каждый объект в системе может выполнять некоторые вредоносные действия.

Все вышеупомянутые методы имеют много недостатков. Они аутентифицируют только пользователей и не аутентифицируют устройства интернета вещей. Они также используют централизованные методы аутентификации. При централизованном методе все вычислительные данные хранятся на сервере. Объекты в системе слишком сильно полагаются на сервер или центральный орган для выполнения желаемых транзакций доступа. Если централизованный орган не имеет достаточную надежность с точки зрения безопасности, то это может нарушить безопасность всей системы.

Чтобы уменьшить недостатки централизованной (доверенной третьей стороной) аутентификации устройств интернета вещей, предлагается децентрализованная схема аутентификации конечного пользователя, устройств интернета вещей и транзакций с использованием алгоритмов, обеспечивающих технологию блокчейн. Предлагаемая система обеспечивает возможность аутентификации конечного пользователя и устройств интернета вещей. Предлагаемая система также облегчает конечным пользователям сопоставление защищенной связи с устройствами интернета вещей, обеспечивая при этом безопасность без каких-либо требований к централизованной идентификации.

Основная цель архитектуры системы, предложенной в данной статье – обеспечить безопасность устройств интернета вещей на аппаратном уровне. Для достижения этой цели необходимо использовать технологию блокчейна.

Архитектура системы

В предлагаемой системной архитектуре есть пять основных объектов с доступом к веб-алгоритмам через интернет: администратор, конечные пользователи, которые обеспечивают прямое подключение к системе, алгоритм блокчейна, база данных (сервер *MySQL)*, содержащая данные конечных пользователей и устройства *IoT*. Более подробное описание объектов приведено ниже. Во время регистрации присваиваются уникальные хэш-адреса (открытый и закрытый ключи) устройствам интернета вещей и конечным пользователям. Как устройства интернета вещей, так и конечные пользователи зарегистрированы в сети интернет. Администратор и базы данных также являются частью системы. Подробная архитектура системы представлена на рис. 2.

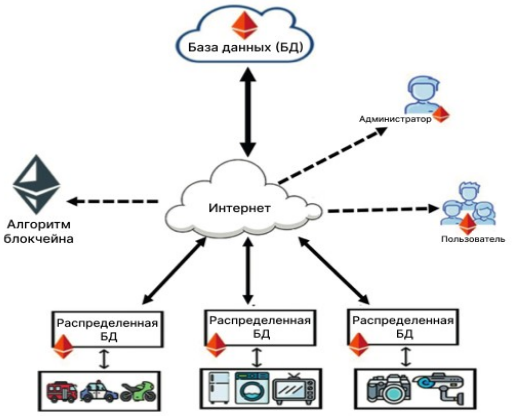

Рисунок 2

Администратор

Администратор является наиболее ценным подразделением системы и отвечает за контроль доступа пользователей, список пользователей, службы устройств интернета вещей и разрешение конечным пользователям на доступ к устройствам интернета вещей. Только владелец конкретной организации или архитектурной системы имеет возможности управления и контроля доступа. Основным клиентом в рамках фреймворка является владелец или создатель алгоритма блокчейна. Владелец алгоритма блокчейна может добавлять устройства интернета вещей по запросу пользователя как часть системы. Администратор также предоставляет конечным пользователям разрешение на доступ к устройствам интернета вещей с помощью алгоритма. Администратор имеет возможность блокировать новые транзакции в системе и добавлять блок в цепочку. Самым первым объектом в системе является администратор, поэтому его блок не имеет предыдущего хэш-значения.

Конечные пользователи

Утилизаторы в рамках системы – это клиенты, которые запрашивают согласие у алгоритма блокчейна на доступ к определенным устройствам интернета вещей. Как только конечным пользователям разрешается получать авторизацию после аутентификации с помощью алгоритма аутентификации, они связываются с назначенным серверным узлом, способным управлять желаемым устройством интернета вещей для аутентификации и доступа.

Алгоритм блокчейна

Алгоритм блокчейна предоставляет аутентифицированному утилизатору доступ к аутентифицированному смарт-устройству. Регистрация конечных пользователей, интеллектуальные устройства, контроль доступа, аутентификация и функциональные возможности развертываются, чтобы стать централизованной архитектурой с помощью алгоритма блокчейна.

База данных

В предложенном прототипе решения база данных используется для контроля доступа к устройствам интернета вещей. База данных хранит устройства интернета вещей, информацию, данные конечного пользователя и вычислительные транзакции в виде общедоступных реестров. База данных распределена между всеми конечными пользователями в форме распределенной бухгалтерской книги, но они не могут изменять, удалять или обновлять какие-либо записи, они могут только создать свою собственную запись транзакции.

Устройства интернета вещей

Ожидается, что интеллектуальные устройства в системе будут ресурсоемкими устройствами с ограниченными возможностями хранения, обработки и памяти.

Взаимодействие между объектами

Взаимодействие между объектами системы происходит в два основных этапа, а именно, онлайн- и оффлайн-взаимодействия. На рис. 3 показана последовательность взаимодействий между конечным пользователем и устройствами интернета вещей для успешной аутентификации пользователя, а также доступа пользователя к устройствам интернета вещей. Безопасный сеанс устанавливается для безопасного соединения между конечными пользователями и

интеллектуальными устройствами. При онлайн-взаимодействии администратор изначально генерирует алгоритм смарт-контракта, регистрирует пользователя в системе и сопоставляет его с сервером *MySQL* с помощью выбранных функций. Уникальные частные и публичные адреса присваиваются пользователям с помощью алгоритмов. Администратор добавляет устройства в систему, а также присваивает уникальные адреса с помощью алгоритмов и сохраняет их на сервере *MySQL*. Вот почему аутентифицированные пользователи могут получить доступ к аутентифицированным устройствам, которые являются частью системы. На рис. 3 представлена схема взаимодействия конечного пользователя и устройств интернета вещей.

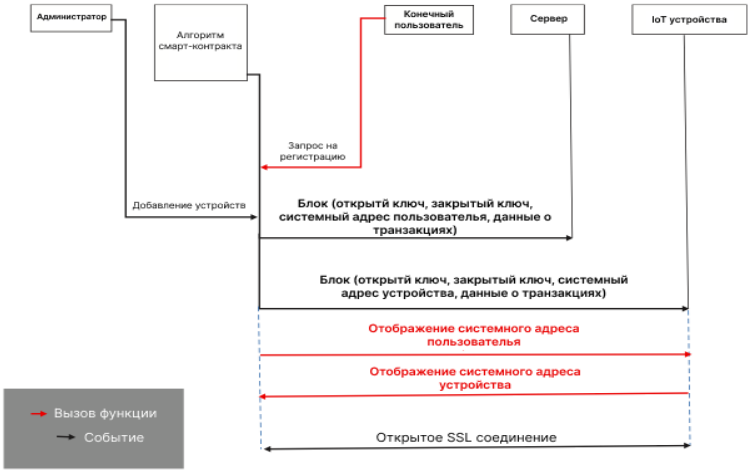

Рисунок 3

Когда пользователь успешно проходит аутентификацию (получает свои уникальные открытый и закрытый ключи) и ему необходимо получить доступ к конкретному устройству интернета вещей, пользователь первоначально передает запрос на аутентификацию алгоритму блокчейна, используя запрос на регистрацию. Алгоритм распознает *SQL*-сервер аутентифицированного смарт-устройства для этого конечного пользователя. Если устройство не аутентифицировано или клиент не имеет права использовать это устройство, то система отклоняет запрос пользователя. В противном случае, если и устройство интернета вещей, и пользователь являются действительными и являются частью системных объектов, алгоритм блокчейна выделит конечному пользователю разрешение на доступ к авторизованному устройству и сохранит информацию о доступе в виде шифрования на сервере *SQL*, а затем передаст ее всем пользователям публично.

Когда пользователь успешно регистрируется в системе с помощью смарт-контракта, алгоритм сохраняет идентификатор пользователя, публичный адрес, личный адрес и предыдущие общедоступные хэш-значения. Генерируется блок, содержащий открытый и закрытый ключи пользователя, транзакционные данные и предыдущие хэш-значения. Публичные и частные адреса пользователей хранятся в виде значений хэш-ключа. Алгоритм хэширования ключей *SHA*-256 используется для генерации значений хэш-ключей. 64-битные значения ключей, генерируемые *SHA*-256, находятся в зашифрованном виде.

Сначала пользователи регистрируются в системе и получают значения открытого и закрытого хэш-ключей, которые хранятся на сервере *SQL*, затем пользователь входит в систему, используя открытый ключ. Смарт-контракт определяет, является ли он действительным пользователем или нет. Если

пользователь не авторизован, его запрос отклоняется с ошибкой, в противном случае – пользователь успешно входит в систему со значениями открытого и закрытого хэш-ключей.

Заключение

В данной статье предложен архитектурный дизайн логических алгоритмов на основе блокчейна с использованием алгоритма значений хэш-ключа для конечных пользователей, устройств интернета вещей и аутентификации транзакций в распределенном виде без вмешательства третьих лиц. Аутентификация большого количества конечных пользователей, устройств интернета вещей и транзакций приводит к развертыванию данных с помощью сервера *MySQ*L, что освобождает конечных пользователей и устройства интернета вещей от вычислительной сложности аутентификации в сети блокчейн. Если распределенный реестр не обновляется после каждой транзакции, происходит потеря данных, что создает вредоносность между блоками распределенного реестра, поскольку каждый блок связан с предыдущим блоком через предыдущее значение открытого хэш-ключа для создания цепочки. В будущем может быть реализована децентрализованная архитектура для обеспечения безопасности устройств интернета вещей на стороне сервера.

Литература

1. Almadhoun R., Kadadha M., Alhemeiri M., Alshehhi M. and Salah K. A user authentication scheme of IoT devices using blockchain-enabled fog nodes 2018, in Proceedings of the 2018 IEEE // ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018. Aqaba, Jordan. – pp. 1-8.
2. Lally G and Sgandurra D. Towards a framework for testing the security of IoT devices consistently, in Proceedings of the First International Workshop on ETAA, 2018, Barcelona, Spain, September.
3. Park N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors (Swit- zerland), 2015. – vol. 16. – pp. 1-16.
4. Mishra S. and Paul A. A critical analysis of attack detection schemes in IoT and open challenges, in Proceedings of the 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON). 2020. Noida, India, October. – pp. 57-62.
5. Luu L., Chu D.H., Olickel H., Saxena P. and Hobor A. Making smart contracts smarter, in Proceedings of the ACM Proceedings // ACM Conference on Computer and Communications Security, 2016. – pp. 254-69.
6. Зараменских Е.П. Интернет вещей. Исследования и область применения. – М.: ИНФРА-М, 2016. – 188 с.
7. Киреева А. И. «Интернет Вещей» И Области Его Использования // Инновационное Развитие, 2017. – Вып. 6 (11). – ISSN 2500-3887.
8. Дрешер Д. Основы блокчейна. – М.: ДМК Пресс, 2018. – 125 с.
9. Alonso A. Fernа́ndez F., Marco L. and Salvachúa J. IAA- CaaS: IoT Application-Scoped Access Control as a Service, Futur Internet, 2017. – vol. 9. – № 4. – p. 64.
10. Ibrahim M. H. Octopus: an edge-fog mutual authentication scheme. International Journal on Network Security, 2016. – vol. 18. – pp. 1089-1101.