ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ДЛЯ ЗАЩИТЫ ДАННЫХ В СЕТЯХ IoT

Абдужаппарова Муборак Балтабаевна
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, доцент кафедры «Телекоммуникационный инжиниринг»
Абдуллаев Абдуфаттох Зафарович
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, магистрант кафедры «Телекоммуникационный инжиниринг»
E-mail: abdufattohabdullaev@gmail.com, +998994868288
https://doi.org/10.5281/zenodo.17935493

Аннотация

В тезисе рассматриваются методы аутентификации, применяемые для защиты данных в сетях Интернета вещей (IoT). Актуальность исследования обусловлена быстрым ростом числа IoT-устройств и повышением требований к обеспечению информационной безопасности в телекоммуникационных системах. Целью работы является анализ существующих методов аутентификации и оценка их эффективности с учётом ограниченных вычислительных и энергетических ресурсов IoT-устройств. В ходе исследования рассмотрены традиционные и современные подходы к аутентификации, включая криптографические и многофакторные методы. Проведён сравнительный анализ методов по критериям безопасности, надёжности и ресурсной эффективности. Полученные результаты позволяют определить наиболее перспективные методы аутентификации для применения в IoT-сетях и могут быть использованы при проектировании защищённых телекоммуникационных систем.

Ключевые слова: Интернет вещей, IoT, аутентификация, защита данных, информационная безопасность, телекоммуникационные сети.

Abstract: This thesis examines authentication methods used to protect data in Internet of Things (IoT) networks. The relevance of the study is determined by the rapid growth in the number of IoT devices and the increasing requirements for information security in telecommunication systems. The aim of the research is to analyze existing authentication methods and evaluate their effectiveness considering the limited computational and energy resources of IoT devices. The study reviews both traditional and modern authentication approaches, including cryptographic and multi-factor methods. A comparative analysis of authentication methods is conducted based on security, reliability, and resource efficiency criteria. The obtained results make it possible to identify the most promising authentication methods for IoT networks and can be applied in the design of secure telecommunication systems.

Keywords: Internet of Things, IoT, authentication, data protection, information security, telecommunication networks.

Основной текст тезиса

В настоящее время технологии Интернета вещей (Internet of Things, IoT) активно внедряются в различные сферы человеческой деятельности, включая телекоммуникации, промышленность, здравоохранение, транспорт и системы «умного города». Количество IoT-устройств и объёмы передаваемых ими данных постоянно

растут, что приводит к повышению требований к обеспечению информационной безопасности. Одной из ключевых проблем в сетях IoT является защита данных от несанкционированного доступа, подмены и утечки информации. В этой связи особую актуальность приобретает задача аутентификации устройств и пользователей в IoT-сетях.

Аутентификация является базовым механизмом информационной безопасности и представляет собой процесс подтверждения подлинности субъекта, запрашивающего доступ к системе или данным. В условиях IoT-сетей аутентификация усложняется рядом факторов, среди которых можно выделить ограниченные вычислительные и энергетические ресурсы устройств, гетерогенность сетевой инфраструктуры, а также масштабируемость и динамичность сети. Традиционные методы аутентификации, широко применяемые в классических телекоммуникационных системах, не всегда подходят для IoT-среды, что требует анализа и адаптации существующих подходов.

Целью данного тезиса является исследование и анализ методов аутентификации, применяемых для защиты данных в сетях Интернета вещей, а также оценка их эффективности с учётом особенностей телекоммуникационных IoT-систем. Для достижения поставленной цели в работе рассматриваются основные типы методов аутентификации и проводится их сравнительный анализ.

В ходе исследования были проанализированы традиционные методы аутентификации, основанные на использовании паролей и идентификаторов, а также более современные подходы, включающие криптографические методы, многофакторную аутентификацию и методы на основе сертификатов. Особое внимание уделено криптографическим методам, использующим симметричное и асимметричное шифрование, так как они обеспечивают более высокий уровень защиты данных. Однако применение сложных криптографических алгоритмов в IoT-сетях может быть ограничено из-за низкой вычислительной мощности и ограниченного энергопотребления устройств.

Также в работе рассмотрены многофакторные методы аутентификации, которые предполагают использование двух и более факторов подтверждения подлинности, таких как знание (пароль), владение (устройство или токен) и биометрические характеристики. Данные методы позволяют повысить уровень безопасности, однако могут увеличивать задержки при передаче данных и усложнять процесс аутентификации, что не всегда допустимо для IoT-приложений реального времени.

Проведён сравнительный анализ методов аутентификации по таким критериям, как уровень безопасности, надёжность, ресурсная эффективность и масштабируемость. Результаты анализа показывают, что универсального метода аутентификации, подходящего для всех IoT-сценариев, не существует. Выбор конкретного метода должен осуществляться с учётом архитектуры сети, типа IoT-устройств, требований к безопасности и характеристик телекоммуникационной инфраструктуры.

В заключение можно отметить, что эффективная аутентификация является необходимым условием обеспечения защиты данных в сетях Интернета вещей. Результаты данного исследования могут быть использованы при проектировании и модернизации защищённых телекоммуникационных IoT-систем, а также при

дальнейшем развитии методов обеспечения информационной безопасности в условиях цифровизации.

Adabiyotlar, References, Литературы:

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey // Computer Networks. – 2010. – Vol. 54, No. 15. – P. 2787–2805.
2. Roman R., Zhou J., Lopez J. On the features and challenges of security and privacy in distributed Internet of Things // Computer Networks. – 2013. – Vol. 57, No. 10. – P. 2266–2279.
3. Sicari S., Rizzardi A., Grieco L. A., Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead // Computer Networks. – 2015. – Vol. 76. – P. 146–164.
4. Alaba F. A., Othman M., Hashem I. A. T., Alotaibi F. Internet of Things security: A survey // Journal of Network and Computer Applications. – 2017. – Vol. 88. – P. 10–28.
5. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.