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

Аннотация: В работе исследуются методы аутентификации, применяемые для обеспечения защиты данных в сетях Интернета вещей (IoT). Актуальность темы обусловлена стремительным увеличением количества IoT-устройств и возрастающими требованиями к уровню информационной безопасности в телекоммуникационных системах. Цель исследования заключается в анализе существующих подходов к аутентификации и оценке их эффективности с учётом ограниченных вычислительных и энергетических ресурсов устройств IoT. В рамках работы рассмотрены как традиционные, так и современные методы аутентификации, включая криптографические и многофакторные решения. Выполнен сравнительный анализ данных методов по показателям безопасности, надёжности и ресурсной эффективности. Полученные результаты позволяют выявить наиболее перспективные подходы к аутентификации для использования в IoT-сетях и могут быть применены при разработке защищённых телекоммуникационных систем.

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

Abstract: This paper examines authentication methods used to ensure data protection in Internet of Things (IoT) networks. The relevance of the study is driven 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 approaches and evaluate their effectiveness, taking into account the limited computational and energy resources of IoT devices. The study considers both traditional and modern authentication methods, including cryptographic and multi-factor solutions. A comparative analysis of these methods is carried out based on security, reliability, and resource efficiency criteria. The obtained results

make it possible to identify the most promising authentication approaches for use in 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) находят широкое применение в различных сферах человеческой деятельности, включая телекоммуникации, промышленность, здравоохранение, транспорт и системы «умного города». Рост числа IoT-устройств, а также увеличение объёмов генерируемых и передаваемых данных обусловливают ужесточение требований к обеспечению информационной безопасности. Одной из ключевых задач в IoT-сетях является защита данных от несанкционированного доступа, подмены и утечки. В связи с этим особую значимость приобретает проблема аутентификации устройств и пользователей в IoT-среде.

Аутентификация представляет собой базовый механизм обеспечения информационной безопасности и определяется как процесс подтверждения подлинности субъекта, запрашивающего доступ к системе или информационным ресурсам. В условиях IoT-сетей реализация аутентификации осложняется рядом факторов, к которым относятся ограниченные вычислительные и энергетические ресурсы устройств, гетерогенность сетевой инфраструктуры, а также высокая масштабируемость и динамичность сети. Традиционные методы аутентификации, широко применяемые в классических телекоммуникационных системах, не в полной мере соответствуют требованиям IoT-среды, что обуславливает необходимость их анализа и адаптации.

Целью настоящего исследования является изучение и анализ методов аутентификации, применяемых для обеспечения защиты данных в сетях Интернета вещей, а также оценка их эффективности с учётом специфики телекоммуникационных IoT-систем. Для достижения поставленной цели в работе рассматриваются основные категории методов аутентификации и выполняется их сравнительный анализ.

В рамках исследования проанализированы как традиционные методы аутентификации, основанные на использовании паролей и идентификаторов, так и современные подходы, включающие криптографические методы, многофакторную аутентификацию и решения на основе сертификатов. Особое внимание уделено криптографическим механизмам, использующим симметричное и асимметричное шифрование, поскольку они обеспечивают более высокий уровень защиты информации. Вместе с тем применение сложных криптографических алгоритмов в IoT-сетях может быть ограничено вследствие

недостаточной вычислительной мощности и ограниченных энергетических ресурсов устройств.

В работе также рассмотрены многофакторные методы аутентификации, предполагающие использование двух и более факторов подтверждения подлинности, включая знания (пароль), владение (устройство или токен) и биометрические характеристики. Применение данных подходов способствует повышению уровня информационной безопасности, однако может приводить к увеличению задержек при передаче данных и усложнению процедуры аутентификации, что ограничивает их использование в IoT-приложениях реального времени.

Выполнен сравнительный анализ методов аутентификации по критериям уровня безопасности, надёжности, ресурсной эффективности и масштабируемости. Результаты исследования свидетельствуют об отсутствии универсального метода, одинаково эффективного для всех сценариев применения IoT. Выбор оптимального решения должен осуществляться с учётом архитектурных особенностей сети, типа используемых устройств, требований к обеспечению безопасности и характеристик телекоммуникационной инфраструктуры.

В заключение следует подчеркнуть, что эффективная реализация механизмов аутентификации является необходимым условием обеспечения защиты данных в сетях Интернета вещей. Полученные в ходе исследования результаты могут быть использованы при проектировании и совершенствовании защищённых телекоммуникационных IoT-систем, а также при дальнейшем развитии методов обеспечения информационной безопасности в условиях цифровой трансформации.

Список использованной 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. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements.