УДК 004.056.53

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ В СИСТЕМАХ ИНТЕРНЕТА ВЕЩЕЙ

Романович Н.Н.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Алексеев В.Ф. – канд.техн.наук, доцент, доцент кафедры ПИКС

Аннотация. В данной статье рассматривается концепция конфиденциальных вычислений и возможности ее применения к Интернету вещей. Показано, что конфиденциальные вычисления обеспечивают защиту данных и кода во время их обработки, что является уязвимостью в традиционных методах обеспечения безопасности. Такие методы, как защищенные анклавы и гомоморфное шифрование, могут использоваться для реализации конфиденциальных вычислений в IoT. Отмечается, что конфиденциальные вычисления могут повысить эффективность приложений IoT, но существуют проблемы, связанные с их реализацией, такие как ограниченная вычислительная мощность и память на устройствах IoT и отсутствие стандартизации в отрасли. В заключение в статье подчеркивается важность изучения новых методов обеспечения безопасности, чтобы гарантировать, что преимущества интернета вещей реализуются не в ущерб безопасности.

Ключевые слова: интернет вещей, конфиденциальные вычисления, кибербезопасность

Введение. В связи с тем, что Интернет вещей (*IoT*) в настоящее время активно развивается, потребность в безопасных и конфиденциальных вычислениях становится все более важной. Конфиденциальные вычисления (англ. *confidential computing*) – это технологии обеспечения безопасности, при использовании которых защищаются от несанкционированного доступа как конфиденциальные данные, так и программный код, их обрабатывающий, во время их использования. В статье рассматривается вопрос, применения конфиденциальных вычислений к Интернету вещей для обеспечения безопасной и конфиденциальной обработки данных [1–10].

Основная часть. Интернет вещей (*IoT*) является сетью физических устройств, транспортных средств, зданий и других объектов, в которые встроены датчики, программное обеспечение и средства связи, что позволяет им собирать данные и обмениваться ими через Интернет. Эта сеть позволяет объектам взаимодействовать друг с другом, создавая среду, в которой устройства можно удаленно отслеживать, контролировать и оптимизировать в режиме реального времени [1].

Интернет вещей может изменить многие аспекты современной жизни, в том числе здравоохранение, сельское хозяйство, транспорт, производство. Однако его внедрение также создает серьезные проблемы, связанные с конфиденциальностью и безопасностью данных, функциональной совместимостью, стандартизацией и масштабируемостью. Устройства интернета вещей становятся все более распространенными, и все, от бытовой техники до промышленного оборудования, подключается к Интернету. Хотя такое подключение имеет много преимуществ, оно также создает новые риски для безопасности. Например, устройства могут быть уязвимы для взлома и других типов кибератак, а собираемые ими данные могут быть конфиденциальными [2-3].

Конфиденциальные вычисления могут помочь решить некоторые из этих проблем, предоставляя безопасную и частную вычислительную среду для устройств интернета вещей.

Конфиденциальные вычисления – это метод, обеспечивающий защиту данных и кода во время их использования [4]. Это отличается от традиционных методов обеспечения безопасности, которые сосредоточены на защите данных, когда они находятся в состоянии покоя (*data-at-rest*) или в пути (*data-in-transit*). Конфиденциальные вычисления обеспечивают защиту данных и кода даже во время их обработки, когда они наиболее уязвимы для атак [4].

Существуют несколько актуальных методов, которые можно использовать для реализации конфиденциальных вычислений в системах интернета вещей. Один из таких методов известен как защищенные анклавы (англ. *secure enclave*). Защищенный анклав — это часть памяти, изолированная от остальной системы, обеспечивающая безопасную среду для конфиденциальных данных и кода. Реализациями этого метода являются такие технологии, как *Intel Software Guard Extensions* (*SGX*) и технология *ARM TrustZone*. Обе технологии создают защищенный анклав, в котором могут выполняться конфиденциальные вычисления, гарантируя, что данные, обрабатываемые внутри анклава, защищены от несанкционированного доступа [5].

Intel SGX обеспечивает аппаратную защиту программных приложений, позволяя им создавать защищенную область в памяти процессора, называемую анклавом. Эта область зашифрована и изолирована от остальной системы, поэтому любой код или данные в этой области защищены от таких атак, как вредоносное ПО, руткиты и даже от системных администраторов. *SGX* обеспечивает дополнительный уровень безопасности, помимо стандартных средств защиты операционной системы [6].

ARM TrustZone – это аналогичная технология, используемая в устройствах на базе *ARM*, которая обеспечивает безопасную изолированную среду внутри процессора. *TrustZone* имеет два режима: безопасный мир и обычный мир. Безопасный мир – это отдельная среда, невидимая для обычного мира, позволяющая обрабатывать конфиденциальные данные и выполнять вычисления с дополнительной защитой. Эта технология на сегодняшний широко используется в мобильных устройствах, где защищенные среды используются для хранения конфиденциальных данных пользователя, таких как биометрическая информация [7].

Intel SGX и ARM TrustZone – важные технологии безопасности, которые используются для защиты конфиденциальных данных в различных устройствах. Они обеспечивают уровень безопасности за пределами операционной системы и программного обеспечения, создавая защищенные анклавы, в которых конфиденциальные вычисления могут выполняться без опасения несанкционированного доступа.

Другой метод, который можно использовать для реализации конфиденциальных вычислений – это гомоморфное шифрование. Гомоморфное шифрование позволяет выполнять вычисления с зашифрованными данными без их предварительной расшифровки. Этот метод особенно полезен для приложений, требующих конфиденциальности данных, таких как здравоохранение и финансовые приложения.

Конфиденциальные вычисления также могут быть использованы для защиты конфиденциальности пользователей в Интернете вещей. Например, устройства умного дома, такие как камеры и микрофоны, могут быть оснащены функциями конфиденциальных вычислений, чтобы обеспечить защиту пользовательских данных. Этого можно достичь с помощью таких методов, как дифференциальная конфиденциальность, которая добавляет шум к данным для защиты конфиденциальности отдельных пользователей.

Помимо обеспечения безопасности и конфиденциальности, конфиденциальные вычисления также могут повысить эффективность приложений интернета вещей. Например, конфиденциальные вычисления можно использовать для анализа конфиденциальных данных без необходимости передачи данных на удаленный сервер. Это может снизить требования к задержке и пропускной способности приложений интернета вещей, повысив их производительность.

Существует также ряд проблем, связанных с внедрением конфиденциальных вычислений в системы интернета вещей. Одной из таких проблем является ограниченная вычислительная мощность и память устройств: методы конфиденциальных вычислений требуют дополнительной вычислительной мощности и памяти, которые могут быть доступны не на всех устройствах. Это затрудняет реализацию конфиденциальных вычислений на определенных устройствах.

Еще одной из проблем является отсутствие стандартизации в отрасли интернета вещей. Существует множество различных устройств и платформ интернета вещей, каждая из кото-

рых имеет свои уникальные требования к безопасности. Это затрудняет стандартизированное внедрение конфиденциальных вычислений во всей экосистеме интернета вещей.

Заключение. Конфиденциальные вычисления могут обеспечить решение рисков безопасности и конфиденциальности, связанных с IoT. Защищая данные и код во время их использования, конфиденциальные вычисления могут гарантировать конфиденциальность и безопасность обработки информации. Хотя существуют некоторые проблемы, связанные с внедрением конфиденциальных вычислений в IoT, преимущества повышенной безопасности, конфиденциальности и эффективности делают его многообещающей областью исследований и разработок. Поскольку интернет вещей продолжает развиваться и расти, важно исследовать новые методы безопасности, такие как конфиденциальные вычисления, чтобы гарантировать, что преимущества IoT реализуются безопасным и конфиденциальным образом.

Список литературы

1. *Atzori, Luigi. The Internet of Things: A survey / Luigi Atzori, Antonio Iera, Giacomo Morabito // Computer Networks. — 2010. — Oct. — Vol. 54, no. 15. — P. 2787–2805.*

2. *Internet of Things (IoT): A vision, architectural elements, and future directions / Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami // Future Generation Computer Systems. — 2013. — Sep. — Vol. 29, no. 7. — P. 1645–1660.*

3. *Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi [et al.] // IEEE Communications Surveys & Tutorials. — 2015. — Vol. 17, no. 4. — P. 2347–2376.*

4. *What is confidential computing? defined and explained . — Mode of access: https://www.fortinet.com/resources/cyberglossary/confidential-computing. — Date of access: 01.03.2023.*

5. *Trusted Execution Environment: What It is, and What It is Not / M. Sabt, M. Achemlal, A. Bouabdallah. // 2015 IEEE Trustcom/BigDataSE/ISPA — 2015.*

6. *A survey of Intel SGX and its applications / Z. Wei [et. Al] //Frontiers of Computer Science. — 2021. — 06. — Vol. 15.*

7. *TrustZone Explained: Architectural Features and Use Cases / B. Ngabonziza [et al.] // 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). – 2016.*

8. *Trusted Execution Environments for Cloud/Fog-based Internet of Things Applications / Dalton Valadares, Newton Will, Marco Spohn [et al.] // Proceedings of the 11th International Conference on Cloud Computing and Services Science. — [S. l.] : SCITEPRESS - Science and Technology Publications, 2021.*

9. *Secure data processing for IoT middleware systems / Gbadebo Ayoade, Amir El-Ghamry, Vishal Karande [et al.] // The Journal of Supercomputing. — 2018. — Nov. — Vol. 75, no. 8. — P. 4684–4709.*

10. *Аналитика IoT данных с использованием сервиса AWS IoT analytics при исследовании загазованности окружающей среды / К. О. Климов [и др.] // BIG DATA and Advanced Analytics = BIG DATA и анализ высокого уровня : сборник научных статей VII Международной научно-практической конференции, Минск, 19-20 мая 2021 года / редкол.: В. А. Богуш [и др.]. – Минск : Бестпринт, 2021. – С. 131–137.*

UDC 004.056.53

APPLICATION OF CONFIDENTIAL COMPUTING TECHNOLOGIES IN INTERNET OF THINGS SYSTEMS

Romanovich N.N.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alexeev V.F. – PhD, associate professor, associate professor of the Department of ICSD

Annotation. This article discusses the concept of confidential computing and how it can be applied to the Internet of Things. It is shown that confidential computing provides protection of data and code during their processing, which is a vulnerability in traditional security methods. Techniques such as secure enclaves and homomorphic encryption can be used to implement confidential computing in IoT. It is noted that confidential computing can improve the efficiency of IoT applications, but there are problems associated with their implementation, such as limited computing power and memory on IoT devices and a lack of industry standardization. The article concludes by emphasizing the importance of exploring new security practices to ensure that the benefits of the Internet of Things are not realized at the expense of security.

Keywords: internet of things, confidential computing, cybersecurity