Александр Анатольевич ЗАХАРОВ[1]
Кирилл Юрьевич ПОНОМАРЁВ[2]
Евгений Сергеевич НЕСГОВОРОВ[3]
Ольга Владимировна НИССЕНБАУМ[4]

УДК 004.7

ПОСТРОЕНИЕ МОДЕЛИ АВТОРИЗАЦИИ ВНЕШНИХ СРЕДСТВ ЗАЩИТЫ АСУ ТП НА БАЗЕ ИНТЕРНЕТА ВЕЩЕЙ

[1] доктор технических наук, заведующий кафедрой информационной безопасности, Тюменский государственный университет
azaharov@utmn.ru

[2] аспирант кафедры информационной безопасности, Тюменский государственный университет
k.y.ponomaryov@utmn.ru

[3] аспирант кафедры информационной безопасности, Тюменский государственный университет
e.s.nesgovorov@utmn.ru

[4] кандидат физико-математических наук, доцент кафедры информационной безопасности, Тюменский государственный университет
o.v.nissenbaum@utmn.ru

Аннотация

Целью работы является построение модели авторизации и контроля доступа внешних устройств автоматизированных систем управления технологическими процессами (АСУ ТП) в соответствии с концепцией интернета вещей для централизованных, распределенных и смешанных конфигураций.

Цитирование: Захаров А. А. Построение модели авторизации внешних средств защиты АСУ ТП на базе Интернета вещей / А. А. Захаров, К. Ю. Пономарёв, Е. С. Несговоров, О. В. Ниссенбаум // Вестник Тюменского государственного университета. Физико-математическое моделирование. Нефть, газ, энергетика. 2017. Том 3. № 1. С. 99-110.
DOI: 10.21684/2411-7978-2017-3-1-99-110

В статье изучается вопрос защиты АСУ ТП с помощью внешних устройств, датчиков, реализующих концепцию Интернета вещей (Internet of Things, IoT). Рассматриваются различные подходы к построению Интернета вещей, приводятся проблемы распределенной структуры IoT и методы их решения. Основными проблемами в случае децентрализованной системы являются: механизмы регистрации и аутентификации, модели авторизации и контроля доступа, схемы онтологии и обнаружения сервисов. Для реализации механизма контроля доступа предлагаются методы атрибутного шифрования, обзор которых приведен в данной статье. Также построен перечень проблем, связанных с использованием атрибутного шифрования (Attribute-Based Encryption, ABE) в распределенных сетях, в частности, в сетях сенсоров IoT. Приведена схема передачи секретных ключей между центрами выдачи атрибутов и конечными устройствами. Узким местом шифрования на основании атрибутов в распределенной сети является управление криптографическими ключами, для решения этого авторами разработан протокол на основе схемы распределения ключей Отвея-Рииса с единым доверенным центром для всех узлов. Общий секретный ключ вырабатывается в процессе регистрации на сервере аутентификации. Рассмотрены методики реализации механизмов построения онтологии распределенной сети и построен пример такой онтологии. Также затрагивается проблема актуализации атрибутов для схем, использующих ABE.

Ключевые слова

Автоматизированные системы управления, информационная безопасность, конфиденциальность, управление доступом, Интернет вещей, распределенные системы.

DOI: 10.21684/2411-7978-2017-3-1-99-110

Введение

Концепция Интернета вещей (англ. Internet of Things, IoT) эволюционирует с течением времени, тем не менее ключевая идея может быть выражена одним предложением: информационная система, в которую интегрированы разнообразные физические сущности. Под сущностями в данном понятии подразумеваются любые устройства, обладающие возможностью передавать данные в вычислительных сетях: смартфоны, компьютеры, разнообразные датчики, сенсоры и т. д. Все эти устройства объединены в единую сеть и способны взаимодействовать друг с другом и внешней средой. Можно привести следующие примеры внедрения IoT [1]: система производственного контроля (анализ данных от датчиков температуры, влажности, шума, вибрации и т. д.), интеллектуальная система мониторинга энергопитания, промышленная автоматизация и др.

Распределенные сети сбора информации через разнообразные датчики находят применение как средство физической защиты внешнего периметра и могут применяться для обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами. В таком случае идея сети Интернета вещей применяется не в самих автоматизированных системах управления, но на объектах, в которых они находятся, с целью по-

строения внешнего периметра защиты. Однако имеется множество проблем и вопросов, присущих IoT, на которых стоит сосредоточить внимание прежде чем переходить к построению предложенных моделей.

Для построения IoT-систем необходимо иметь в виду их свойства, которые наиболее полно были описаны в [4]:

- разнородность: чаще всего IoT-сети состоят из компонент различных производителей, которые при совместной работе не должны нарушать функциональность системы;
- ограничения по ресурсам: большинство узлов обладают малыми характеристиками памяти и мощности, а большинство каналов связи — низкой пропускной способностью;
- объемы данных: большое количество датчиков и сенсоров в системе может привести к накоплению огромных объемов информации;
- масштабируемость: в IoT-системах большое количество узлов, поэтому их динамическое добавление или удаление не должно нарушать общую функциональность;
- автоматический контроль: компоненты IoT устанавливают связи спонтанно и обладают свойствами самоорганизации для адаптации к условиям.

Особое внимание в научно-исследовательской литературе уделяется вопросам контроля доступа в сетях IoT: необходимость детального и гранулированного контроля информации, возможность учитывать местоположение, ограниченность вычислительных ресурсов.

Наиболее часто IoT-система имеет распределенную архитектуру: все объекты сети могут извлекать, обрабатывать, комбинировать и предоставлять другим объектам различную информацию. В сетях сбора данных все сенсоры способны взаимодействовать друг с другом. Распределенная сеть, позволяющая связывать между собой гетерогенные устройства, представляет собой платформу для создания сложных программных продуктов. Для построения такой структуры необходимо дать ответы на следующие вопросы:

- каким образом производить аутентификацию в динамических условиях и при наличии большого количества устройств?
- каким должен быть механизм контроля доступа?
- каким образом поставщики и обработчики данных узнают друг о друге и получают сетевые и веб-адреса?
- каким образом обеспечить связность в условиях гетерогенности элементов сети и при разных схемах взаимодействия?

Основная часть

Контроль доступа является важнейшей задачей информационной безопасности для любых информационных систем, в том числе и для вычислительных сетей, содержащих датчики и сенсоры сбора данных. В связи с возрастающей тенденцией интеллектуализации датчиков появляется необходимость в распределении доступа на прикладном уровне модели взаимодействия, обеспечива-

ющем поддержку прикладных процессов и управление различными сетевыми объектами.

В распределенных сетях возможно построение схемы контроля доступа на основе атрибутного шифрования (англ. Attribute-Based Encryption, ABE). Впервые ABE-схемы были рассмотрены в статье [9]. При построении систем с ABE шифрованием определяется множество атрибутов, по которым регулируется доступ к информации. Каждое передаваемое в системе сообщение обладает неким набором значений атрибутов. В ключе каждого пользователя зашифровано дерево доступа, указывающее значения набора атрибутов. Проверяется соответствие между значениями атрибутов ключа и данных. Если атрибуты пакета удовлетворяет ключу пользователя, то он может расшифровать сообщение. Такой подход носит название Key Policy (KP-ABE). Ключи пользователям выдает доверенный центр, он же проверяет подлинность значений атрибутов, то есть что пользователи действительно ими обладают. Другая методика Ciphertext Policy (CP-ABE): дерево доступа шифруется в пакет данных, а ключ пользователя включает в себя атрибуты проверки.

Рассмотрим следующую модель контроля доступа: устройства (сенсоры, датчики, исполнительные механизмы) регистрируются на сервере аутентификации *SA* (англ. Authentication Server), генерируя общий секретный ключ. На нем же они проходят процедуру аутентификации. Центры выдачи атрибутов *AA* (англ. Attribute Authority) проводят те же самые операции. Таким образом, каждый узел системы и каждый доверенный центр имеют общий секретный ключ с *SA*. Контроль доступа достигается с помощью применения атрибутного шифрования, так как все сообщения между устройствами шифруются секретными ключами на основе структуры доступа. Атрибутами можно считать различные характеристики конечных устройств или прикладной области. Необходимо рассмотреть схему раздачи ключей от доверенных центров к сенсорам, так как в динамичной среде атрибуты могут меняться, и в ответ на новые изменения возникает необходимость получения нового секретного ключа. Мы опишем этот процесс с использованием протокола Отвея-Рииса [8]. Будем предполагать, что *AA* имеет некий механизм проверки подлинности нового набора атрибутов, а их передачу инициирует само устройство.

1. Устройство отправляет *AA* номер сессии, сгенерированное псевдослучайное число и зашифрованные на общем с *SA* ключе набор атрибутов.

$$N \rightarrow AA\colon I, N, AA, E_N(R_N, attr_{new}, I, N, AA).$$

2. Центр атрибутов передает полученное зашифрованное сообщение *SA*, а также шифрует на их общем ключе свое псевдослучайное число.

$$AA \rightarrow SA\colon I, N, AA, E_N(R_N, attr_{new}, I, N, AA), E_A(R_A, I, N, AA).$$

3. *SA* расшифровывает полученные сообщения, извлекает параметры (*I*, *N*, *AA*) и проверяет их равенство с теми, что были переданы в открытом виде. Если значения не совпадут, он должен прервать протокол или направить запрос на повторную отправку. Также он генерирует общий сеансовый ключ

для *N* и *AA*. Из сообщения от *N* он извлекает атрибуты и подпись и передает их *AA*.

$$SA \rightarrow AA\colon I, E_N(K, R_N, attr_{new}), E_A(K, R_A, attr_{new}).$$

4. На данном шаге АА проверяет равенство полученного случайного числа сгенерированному ранее, проверяет номер сессии. Далее он формирует по полученным атрибутам новый ключ схемы шифрования на основе атрибутов. Передает его *N*, зашифровав симметричным шифром с использованием полученного от *SA* сеансового ключа. Здесь *AA* может удостовериться, что *SA* именно тот, за кого себя выдает — иначе он бы не смог расшифровать сообщение и вернуть тоже псевдослучайное число.

$$AA \rightarrow N\colon I, E_N(K, R_N, attr_{new}), E_K(K_{ABE}).$$

5. Устройство расшифровывает сообщения. С помощью сеансового ключа извлекает ключ, содержащий дерево доступа (KP-ABE) или же сами атрибуты (CP-ABE). Также необходимо проверить на соответствие предыдущим значениям набор атрибутов. *N* удостоверяется, что *SA* именно тот, за кого себя выдает, проверив псевдослучайное число. Можно отправить *AA* ответное сообщение о доставке.

Несмотря на широкое обсуждение возможностей и моделей атрибутного шифрования в научной литературе, многие вопросы до сих пор остаются открытыми и ждут своего решения:

— Как проверять подлинность атрибутов при генерации секретного ключа?
— Каким образом осуществлять безопасную передачу секретных ключей в динамичной и открытой среде?
— Какой должна быть схема, лишенная недостатков, присущих самому атрибутному шифрованию? Например, как исключить возможность

Таблица 1 *Table 1*

Используемые обозначения **Notations used in the article**

N	Узел, который запрашивает новый ключ при изменении значений атрибутов
AA	Доверенный центр, отвечающий за раздачу ключей на основе атрибутов
SA	Доверенный центр, отвечающий за обмен ключами между *AA* и *N*
I	Идентификационный номер сессии
E	Симметричный алгоритм шифрования
K_{ABE}	Ключ криптосистемы ABE, на основе новых атрибутов устройства N
attr	Набор атрибутов и их значений
R	Случайное число
K	Сеансовый ключ

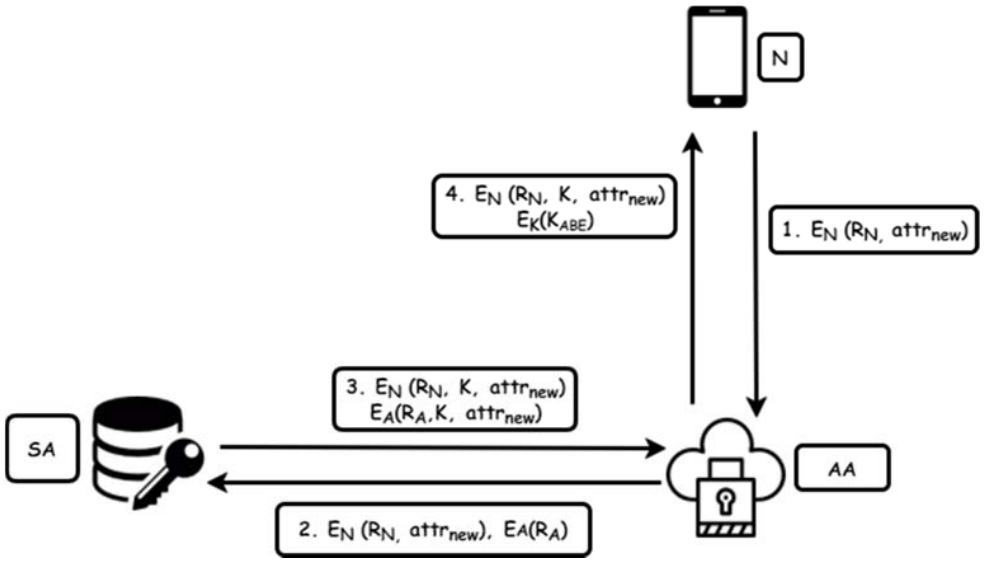

Рис. 1. Протокол Отвея-Рииса *Fig. 1.* Otway-Rees protocol

разделения ключа пользователем и передачи его частей другим участникам?

— Каким образом скрывать в CP-ABE схемах не только сообщение, защищенное секретным ключом, но и сами атрибуты участников и сообщений?

Стоит также отметить, что описано большое количество видов атрибутного шифрования [5-7; 10; 13], в том числе имеются работы, посвященные применению атрибутного шифрования в IoT [12; 14]. Все они реализуют различные подходы к преобразованию информации, но отсутствует единое описание, которое бы объединяло преимущества всех из них. Большую роль также играет вычислительная сложность и затраты на используемую память описанных на текущий момент схем.

В связи с высокими темпами развития концепции Интернета вещей количество новых подключаемых устройств растет экспоненциально. Это создает весьма очевидную проблему: онтология сети неизвестна и очень динамично меняется. В связи с этим возможны ситуации, когда обслуживающие приложения и сервисы становятся недоступны. Также приложения могут не найти требуемые устройства в связи с их недоступностью: например, при неполадке или просто изменении геопозиции [3; 11].

Для решения этой задачи предлагается использовать специальную программную сущность, которая будет хранить текущую онтологию и обрабатывать все запросы в системе. Данные об объекте можно дополнять специальными полями для упрощения работы сервиса, например, хранить его атрибуты (если они не составляют конфиденциальную информацию). При регистрации нового сенсора вся информация о нем: уникальный URI, сегмент подсети, в котором он располагается, и т. д. — сохраняется в базах данных. Далее, когда с приложения бизнес-

логики поступает запрос, например, получение данных или конфигурации с датчиков, изменение состояния, он переадресовывается на наш программный сервис, где возможна дополнительная авторизация, проверка прав доступа на выполнение требуемой операции, и в случае отсутствия нарушений сервис возвращает информацию о логическом или физическом расположении запрашиваемого объекта.

В случае распределенной системы каждая подсеть для обеспечения гибкости и масштабируемости может иметь собственный экземпляр сущности. В таком случае возникает сложность с распределением информации между всеми узлами системы и поддержания ее актуальности. В качестве одного из возможных способов можно реализовать идею протоколов маршрутизации, группируя информацию о хостах по набору определяемых параметров и транслировать ее между связанными сущностями. В такой схеме очень критичной является проблема поддержания актуальности данных, рассмотрение которой заслуживает отдельного глубокого анализа.

Вопрос актуализации, то есть аутентифицированного обновления атрибутов устройства, так или иначе ставится во всех прикладных исследованиях ABE. Существуют различные подходы к решению этой проблемы, начиная с довольно наивных, таких как ведение централизованных списков атрибутов, до весьма сложных схем, позволяющих подтверждать обновление атрибутов различными супервайзерами в рамках их полномочий на изменение того или иного атрибута [2]. В IoT с децентрализованной структурой представляется целесообразным применение последнего подхода.

Заключение

Современные вычислительные сети, такие как Интернет вещей, могут использоваться как система физической защиты производственных объектов. В таком случае они будут представлять собой распределенную сеть сбора и анализа данных от всевозможных датчиков и сенсоров. В статье были описаны проблемы распределенного подхода к построению Интернета вещей, который является наиболее эффективным, с точки зрения его возможностей, и в то же время наиболее сложным в реализации. Самыми главными проблемами такого подхода являются: механизмы регистрации и аутентификации, модели авторизации и контроля доступа, схемы онтологии и, более конкретно, обнаружения сервисов. Присущие Интернету вещей свойства — большое количество устройств и динамический характер взаимодействия между ними — порождают дополнительные вопросы масштабируемости, отказоустойчивости и управления. Для построения системы контроля доступа было предложено использование атрибутного шифрования, приведена модель распространения секретных ключей в условиях большого количества устройств и доверенных центров. К достоинствам атрибутного шифрования безусловно можно отнести гибкую настройку структур доступа. ABE позволяет шифровать сообщение между всеми устройствами сети, но в то же время ситуация, когда знание атрибутов каждого из них не является секретным, может вызвать риски конфиденциальности для особых прикладных областей.

Узким местом шифрования на основании атрибутов в распределенной сети является управление криптографическими ключами, для решения этого было предложено использовать протокол Отвея-Рииса с единым доверенным центром для всех узлов. Это несомненно плюс: каждой сущности необходимо хранить лишь один ключ для связи с этим доверенным центром, но также такая схема несомненно порождает риски отказоустойчивости из-за единого узла связи. Общий секретный ключ вырабатывается в процессе регистрации на таком доверенном центре — сервере аутентификации. Также был описан один из вариантов модели построения онтологии сети. В дальнейшем планируется реализация программного прототипа для построения реальной системы, выявления возможных недостатков.

СПИСОК ЛИТЕРАТУРЫ

1. Куприяновский В. П. Интернет Вещей на промышленных предприятиях / В. П. Куприяновский, Д. Е. Намиот, В. И. Дрожжинов, Ю. В. Куприяновская, М. О. Иванов // International Journal of Open Information Technologies. 2016. Том 4. № 12. С. 69-78.
2. Chase M. Multi-authority attribute based encryption / M. Chase // Theory of Cryptography Conference. Springer Berlin Heidelberg. 2007. Pp. 515-534. DOI: 10.1007/978-3-540-70936-7_28
3. Hachem S. Ontologies for the internet of things / S. Hachem, T. Teixeira, V. Issarny // Proceedings of the 8th Middleware Doctoral Symposium. ACM. 2011. Pp. 3. DOI: 10.1145/2093190.2093193
4. Leloglu E. A. Review of Security Concerns in Internet of Things / E. A. Leloglu // Journal of Computer and Communications. 2017. No 5. Pp. 121-136.
5. Lewko A. Decentralizing attribute-based encryption / A. Lewko, B. Waters // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg. 2011. Pp. 568-588. DOI: 10.1007/978-3-642-20465-4_31
6. Lewko A. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption / A. Lewko, A. Sahai, T. Okamoto, K. Takashima, B. Waters // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg. 2010. Pp. 62-91. DOI: 10.1007/978-3-642-13190-5_4
7. Ostrovsky R. Attribute-based encryption with non-monotonic access structures / R. Ostrovsky, A. Sahai, B. Waters // Proceedings of the 14th ACM conference on Computer and communications security. ACM. 2007. Pp. 195-203. DOI: 10.1145/1315245.1315270
8. Otway D. Efficient and Timely Mutual Authentication / D. Otway, O. Rees // Operating Systems Review. 1987. Vol. 24. No 1. Pp. 8-10. DOI: 10.1145/24592.24594
9. Sahai A. Fuzzy Identity-Based Encryption / A. Sahai, B. Waters // Advances in Cryptology V Eurocrypt. 2005. Pp. 457-473. DOI: 10.1007/11426639_27
10. Wang G. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services / G. Wang, Q. Liu, J. Wu // Proceedings of the 17th ACM conference

on Computer and communications security. ACM. 2010. Pp. 735-737. DOI: 10.1145/1866307.1866414

11. Wang W. A comprehensive ontology for knowledge representation in the internet of things / W. Wang, S. De, R. Toenjes, E. Reetz, K. Moessner // Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE. 2012. Pp. 1793-1798. DOI: 10.1109/trustcom.2012.20
12. Wang X. Performance evaluation of attribute-based encryption: Toward data privacy in the IoT / X. Wang, J. Zhang, E. M. Schooler, M. Ion // Communications (ICC), 2014 IEEE International Conference on. IEEE. 2014. Pp. 725-730. DOI: 10.1109/icc.2014.6883405
13. Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization / B. Waters // International Workshop on Public Key Cryptography. Springer Berlin Heidelberg. 2011. Pp. 53-70. DOI: 10.1007/978-3-642-19379-8_4
14. Yao X. A lightweight attribute-based encryption scheme for the Internet of Things / X. Yao, Z. Chen, Y. Tian // Future Generation Computer Systems. 2015. Vol. 49. Pp. 104-112. DOI: 10.1016/j.future.2014.10.010

Aleksandr A. ZAKHAROV[1]
Kirill Yu. PONOMAREV[2]
Evgeniy S. NESGOVOROV[3]
Olga V. NISSENBAUM[4]

CONSTRUCTION OF THE AUTHORIZATION MODEL OF THE EXTERNAL MEANS OF PROTECTION OF AUTOMATED MANAGEMENT SYSTEMS OF TECHNOLOGICAL PROCESSES BASED ON THE INTERNET OF THINGS

[1] Dr. Sci. (Tech.), Head of the Information Security Department,
Tyumen State University
azaharov@utmn.ru

[2] Postgraduate Student, Information Security Department,
Tyumen State University
k.y.ponomaryov@utmn.ru

[3] Postgraduate Student, Information Security Department,
Tyumen State University
e.s.nesgovorov@utmn.ru

[4] Cand. Sci. (Phys.-Math.), Associate Professor,
Information Security Department, Tyumen State University
o.v.nissenbaum@utmn.ru

Abstract

The aim of the work is to build the model of authorization and the access control of the external devices of automated control systems by technological processes in accordance with the concept of the Internet of Things for centralized, distributed and mixed configurations.

The article studies the issue of protection of the automated control systems by technological processes with the help of external devices, sensors that implement the concept of Internet

Citation: Zakharov A. A., Ponomarev K. Yu., Nesgovorov E. S., Nissenbaum O. V. 2017. "Construction of the Authorization Model of the External Means of Protection of Automated Management Systems of Technological Processes Based on the Internet of Things". Tyumen State University Herald. Physical and Mathematical Modeling. Oil, Gas, Energy, vol. 3, no 1, pp. 99-110.
DOI: 10.21684/2411-7978-2017-3-1-99-110

of Things (IoT). Various approaches to the construction of the Internet of Things are considered, problems of the distributed IoT structure and methods for their solution are presented. The main problems in the case of a decentralized system are: registration and authentication mechanisms, authorization and access control models, and the schemes of ontology and the service detection. To implement the access control mechanism, we propose the methods of attribute encryption, the review of which is given in this article. Also, a list of problems associated with the use of Attribute-Based Encryption (ABE) in distributed networks, in particular, in the networks of sensors IoT, is constructed. The scheme for the transfer of secret keys between the centers of issuing attributes and end devices is given. The bottleneck of the encryption based on attributes in a distributed network is the cryptographic keys management. To solve this problem the authors developed the protocol based on the Otway-Rees protocol key distribution scheme with a single trusted center for all nodes. The shared secret key is generated during the registration process on the authentication server. Methods for implementing mechanisms for constructing the ontology of a distributed network are considered, and an example of such ontology is constructed. Also, the problem of the attributes actualization for schemes using ABE is discussed.

Keywords

Internet of Things, IoT, information security, authentication, confidentiality, access control, distributed systems.

DOI: 10.21684/2411-7978-2017-3-1-99-110

REFERENCES

1. Kupriyanovskiy V. P., Namiot D. E., Drozhzhinov V. I., Kupriyanovskaya Yu. V., Ivanov M. O. 2016. “Internet Veshchey na promyshlennykh predpriyatiyakh” [Internet of Things in Industrial Enterprises]. International Journal of Open Information Technologies, vol. 4, no 12, pp. 69-78.
2. Chase M. 2007. “Multi-authority Attribute Based Encryption”. Theory of Cryptography Conference, Springer Berlin Heidelberg, pp. 515-534. DOI: 10.1007/978-3-540-70936-7_28
3. Hachem S., Teixeira T., Issarny V. 2011. “Ontologies for the Internet of Things”. Proceedings of the 8th Middleware Doctoral Symposium, ACM, pp. 3. DOI: 10.1145/2093190.2093193
4. Leloglu E. A. 2017. “Review of Security Concerns in Internet of Things”. Journal of Computer and Communications, no 5, pp. 121-136.
5. Lewko A., Waters B. 2011. “Decentralizing attribute-based encryption”. Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 568-588. DOI: 10.1007/978-3-642-20465-4_31
6. Lewko A., Sahai A., Okamoto T., Takashima K., Waters B. 2010. “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption”. Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 62-91. DOI: 10.1007/978-3-642-13190-5_4

7. Ostrovsky R., Sahai A., Waters B. 2007. "Attribute-Based Encryption with Non-Monotonic Access Structures". Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, pp. 195-203. DOI: 10.1145/1315245.1315270
8. Otway D., Rees O. 1987. "Efficient and Timely Mutual Authentication". Operating Systems Review, vol. 24, no 1, pp. 8-10. DOI: 10.1145/24592.24594
9. Sahai A., Waters B. 2005. "Fuzzy Identity-Based Encryption". Advances in Cryptology V Eurocrypt, pp. 457-473. DOI: 10.1007/11426639_27
10. Wang G., Liu Q., Wu J. 2010. "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services". Proceedings of the 17th ACM Conference on Computer and Communications Security, ACM, pp. 735-737. DOI: 10.1145/1866307.1866414
11. Wang W., De S., Toenjes R., Reetz E., Moessner K. 2012. "A Comprehensive Ontology for Knowledge Representation in the Internet of Things". Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, IEEE, pp. 1793-1798. DOI: 10.1109/trustcom.2012.20
12. Wang X., Zhang J., Schooler E. M., Ion M. 2014. "Performance Evaluation of Attribute-Based Encryption: Toward Data Privacy in the IoT". Communications (ICC), 2014 IEEE International Conference on, IEEE, pp. 725-730. DOI: 10.1109/icc.2014.6883405
13. Waters B. 2011. "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization". International Workshop on Public Key Cryptography, Springer Berlin Heidelberg, pp. 53-70. DOI: 10.1007/978-3-642-19379-8_4
14. Yao X., Chen Z., Tian Y. 2015. "A Lightweight Attribute-Based Encryption Scheme for the Internet of Things". Future Generation Computer Systems, vol. 49, pp. 104-112. DOI: 10.1016/j.future.2014.10.010