СИСТЕМА ПОИСКА ПО ОБРАЗЦАМ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ «ИНТЕРНЕТА ВЕЩЕЙ» И «ИНТЕРНЕТА ВСЕГО»

Козлов А.С.[1], Дудник С.В.[2], Култазин Н.М.[3]
Email: Kozlov1174@scientifictext.ru

[1]Козлов Александр Сергеевич - старший системный администратор,
Филиал
Корпорация «Алайн Текнолоджи Ресерч энд Девелопмент, Инк»;
[2]Дудник Сергей Викторович - ведущий эксперт,
департамент инфраструктурных решений,
ПАО Сбербанк,
г. Москва;
[3]Култазин Нурлан Муратович - инженер инфраструктуры,
Astana International Exchange,
г. Нур-Султан, Республика Казахстан

Аннотация: *рассмотрены особенности поиска по образцам кодовых последовательностей в рамках концепции «Интернета вещей», модель которой представлена в виде системы датчиков смарт-устройств, объединенной единой коммуникационной сетью. Выделены ключевые вопросы безопасной и конфиденциальной передачи данных в информационных системах на базе «Интернета вещей» и «Интернета всего», показан приоритет в данной области атрибутивного кодирования. Предложена модель атрибутивного поиска по ключевым словам, которая базируется на алгоритмах облегченного декодирования и мультиавторизации. Показано, что на основе данного подхода возможно построение методологической базы разработки алгоритмов мультивариантного поиска по ключевым словам. Анализ эффективности работы алгоритмов данного класса был оценен через параметры точности и времени выполнения пользовательских запросов, а также нагрузку на вычислительную мощность аппаратного комплекса информационной системы.*
Ключевые слова: *Интернет вещей, Интернет всего, атрибутивное кодирование, алгоритмы поиска по ключевым словам, облегченное декодирование, мультиавторизация, мультивариантный поиск по ключевым словам.*

CODE SEQUENCES SEARCH SYSTEM FOR THE “INTERNET OF THINGS” AND “INTERNET OF EVERYTHING”

Kozlov A.S.[1], Dudnik S.V.[2], Kultazin N.M.[3]

[1]Kozlov Aleksandr Sergeevich - Senior System Administrator,
"ALIGN TECHNOLOGY RESEARCH AND DEVELOPMENT INCORPORATED",
EMEA RUSSIAN REGION;
[2]Dudnik Sergei Victorovich - Leading Expert,
DEPARTMENT OF INFRASTRUCTURE SOLUTIONS,
PJSC SBERBANK,
MOSCOW;
[3]Kultazin Nurlan Muratovich - Infrastructure Engineer,
ASTANA INTERNATIONAL EXCHANGE, NUR-SULTAN, REPUBLIC OF KAZAKHSTAN

Abstract: *peculiarities code sequences’ samples search within the framework of the “Internet of Things” concept are considered, the model presents system of smart device sensors combined within a single communication network. The key issues of safe and confidential data transmission in information systems based on the “Internet of Things” and “Internet of Everything” are highlighted, the priority in this area of attribute based encryption is shown. A model of attributive search by keywords based on lightweight decryption and multi-authorization algorithms is proposed. It is shown that, based on this approach, it is possible to build a methodological base for the development of multivariate keyword search algorithms. Analysis of the efficiency of the mentioned algorithms was evaluated through the parameters of accuracy and execution time of user queries, as well as the load on the computing power of the hardware complex of the information system.*
Keywords: *Internet of Things, Internet of Everything, attribute based encryption, keyword search algorithms, lightweight decryption, multi-authority, multi-keyword search.*

УДК 004.056

Введение

Появление парадигмы Интернета вещей (Internet of Things, IoT) и Интернета всего (Internet of Everything, IoE) связано с экспоненциальным ростом количества и вычислительным мощностей

мобильных смарт-устройств, бытовой автоматизированной техники и промышленной электроники, а также пропускной способности локальных и глобальных сетей. Однако, одновременно с очевидными преимуществами, которые связаны с внедрением данного подхода, IoT и IoE характеризуются высоким уровень информационных потерь, которые в первую связаны с неавторизованным доступом к передаваемым данным сторонних пользователей. Таким образом, на сегодняшний день одно из заданий построения стратегии защиты информационных сетей связано с кодированием данных на этапе предшествующем их передачи в систему облачного сервиса, что определяет ***актуальность*** данного исследования.

Анализ последних исследований и публикаций показал, что традиционные схемы шифрования с открытым ключом не подходят для распределенных сред IoT и IoE [1, 2, 5, 8]. Перспективным подходом, позволяющим реализовать точное управление доступом к данным в облачном хранилище, является атрибутивное кодирование (attribute based encryption, ABE). Схемы ABE подразделяются на два типа [1, 3, 6, 9, 10]:

- политика безопасности атрибутивного кодирования, представленная на базе криптографического кода (ciphertext-policy, CP);
- политика открытого ключа (key-policy, KP).

В работах [2, 3, 6] показано, что использование CP-ABE в IoT и IoE более продуктивно при проектировании системы контроля доступа к облачному сервису [11, 12, 16-21]. Отдельной задачей является обеспечение надежной работы облачного сервиса в условиях мультиавторизации (multi-authority, MA), что связано с решением нетривиальной задачи обеспечения конфиденциальности передачи данных [6, 13, 22]. Для построения модели атрибутивного кодирования были рассмотрены алгоритмы поиска по ключевым словам (keyword search algorithms, KSA) [4, 7, 15], в частности мультивариантный поиск по ключевым словам (multi-keyword search, MKS) [14, 23, 24]. Также исследования указали на то, что с целью уменьшения нагрузки на вычислительную мощность аппаратного комплекса информационной системы актуально применять в KSA методов облегченного декодирования (lightweight decryption, LD) [1, 25].

Проведенный анализ показал отсутствие целостной методологии в области кодированием данных на этапе предшествующем их передачи в систему облачного сервиса с целью обеспечения безопасности работы информационной системы, что было выделено как **нерешенную часть общей проблемы**.

Целью работы, таким образом, стало построение методологической базы разработки алгоритмов атрибутивного кодирования на мультивариантного поиска по ключевым словам.

1. Методология обеспечения мультиавторизационного доступа к данным облачного сервиса

Как было показано выше современные подходы, которые используются при обеспечении эффективного и защищенного доступа к данным облачного сервиса включают в себя методы атрибутивного кодирования на базе криптографического кода (CP-ABE), алгоритмы мультивариантного поиска по ключевым словам (MKSA), мультиавторизационный подход доступа (MA) и принципы облегченного декодирования (LD). Базовая схема поиска и передачи данных с учетом стратегии предотвращения информационных потерь для облачного сервиса, который базируется на концепциях IoT и IoE, может быть представлена в том виде, что показан на рис. 1.

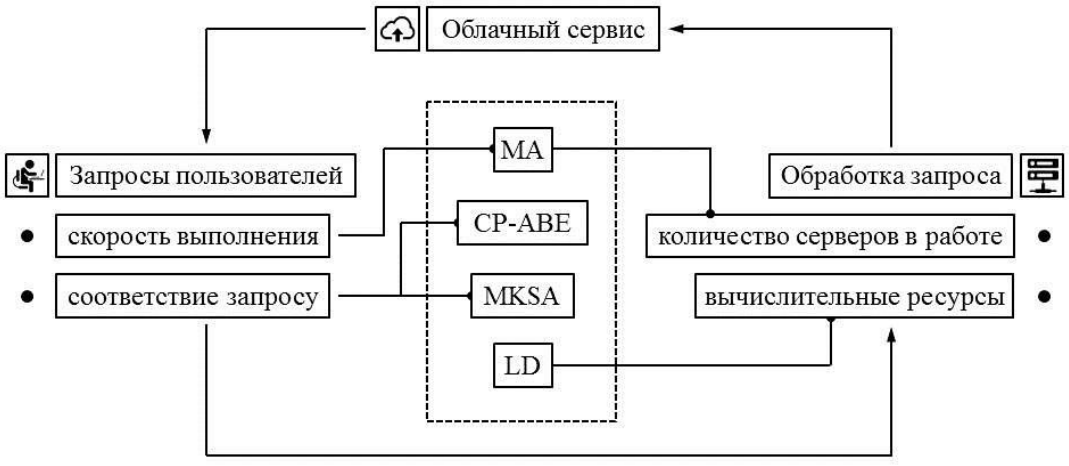

Рис. 1. Схема обеспечения мультиавторизационного доступа к данным облачного сервиса

Соответственно, в рамках системы алгоритмы MKSA и CP-ABE позволяют осуществить поиск по набору ключевых слов, который максимально соответствует запросу пользователя и передать его с полным обеспечением конфиденциальности. При этом за снижение нагрузки на вычислительные

ресурсы аппаратно-программной платформы поиска отвечает функциональный блок LD. Доступ на уровне MA приводит к децентрализации ABE и исключает потребность в центральном блоке авторизации, как уязвимого звена с максимальной нагрузкой, что с одной стороны снижает нагрузку на ресурсы сети, а с другой увеличивает безопасность системы в целом.

Таким образом, прогнозируя работу предложенной схемы обеспечения доступа к данным облачного сервиса можно предположить высокие показатели функциональности, надежности и практичности использования в среде IoT и IoE.

2. Принципы построения модели поиска и передачи данных при работе с облачным сервисом

Для дальнейшего построения математической модели работы системы поиска и передачи данных в соответствии с указанной схемой (рис. 2) необходимо ввести термины для следующих функциональных элементов и обозначить особенности взаимодействия между ними:

- агрегатор данных сенсорных узлов IoT (sensor nodes data owner, SNDO);
- центр сертификации IoT (certificate authority, CA);
- атрибутивный центр (attribute authority, AA)
- облачный сервер (Cloud Server, CS);
- вспомогательный облачный сервер (auxiliary cloud server, ACS);
- пользователь данных IoT с глобальным идентификатором (global user identity, GUID).

Агрегаторы данных сенсорных узлов собирают данные локальных сетей типа «умный дом», «умная фабрика», дистанционное медицинское обслуживание, которые в рамках парадигмы IoT могут взаимодействовать между собой путем передачи данных через облачный сервис. Центр сертификации генерирует начальный набор эталонных параметров адреса и GUID для авторизованных пользователей. Атрибутивные центры при этом генерируют и передают пользователю открытые атрибутивные ключи (attribute public key, APK) и закрытые атрибутивные ключи (attribute secret key, ASK) для каждого из атрибутов.

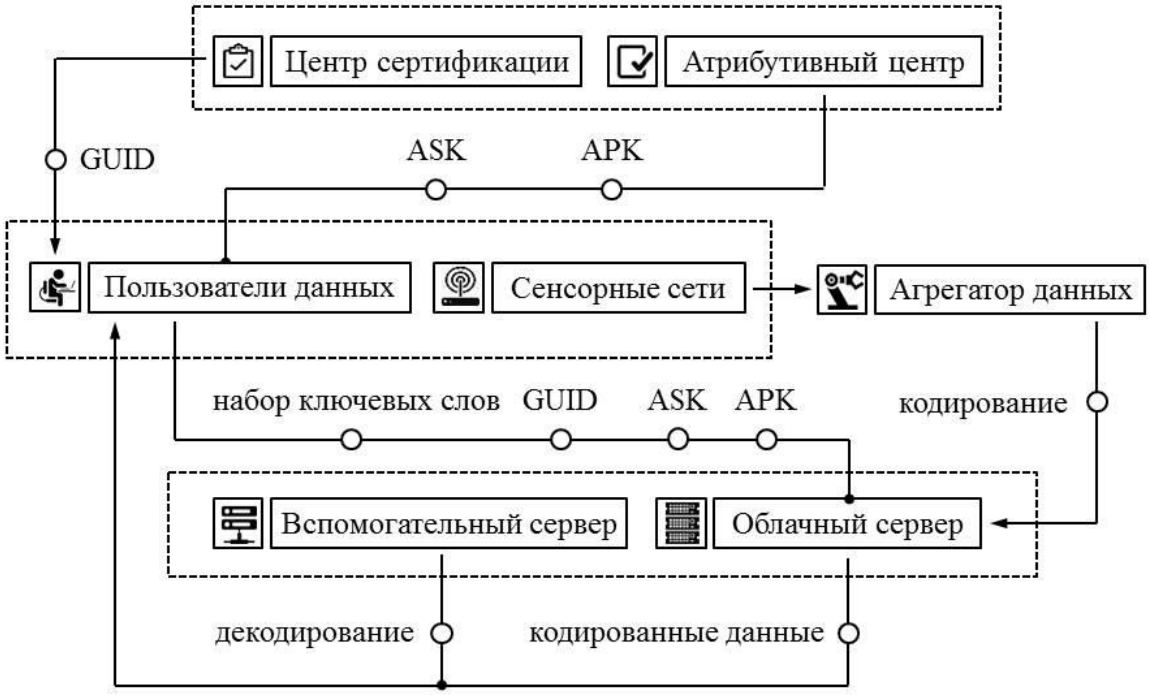

Рис. 2. Модель работы системы поиска и передачи данных облачного сервиса в рамках концепции IoT

Облачный сервер информационной емкостью для хранения больших объемов данных предоставленных пользователями вычислительной мощностью, необходимой для кодирования и декодирования данных, а также выполнения запросов по ключевым словам. Политики безопасности функционирования облачного сервиса при этом подразумевают, что CS будет придерживаться тактики «honest-but-curious», т.е. получать максимум информации о пользователе, как функциональном узле общей схемы, не нарушая при этом договоренностей. В свою очередь вспомогательный облачный сервер выполняет вычисления по декодированию данных, передаваемых пользователю на базе ASK, который формируется через эталонные параметры адреса, для каждого пользователя с GUID. Для поиска данных в кодированном тексте пользователь передает в систему поиска набор ключевых слов и ASK, на основе которых вычисляется код доступа.

3. Математическая модель работы системы поиска и передачи данных облачного сервиса в рамках концепции IoT

На уровне построения математического аппарата функция общей настройки системы поиска и передачи данных может быть представлена через определение на базе параметра стойкости протокола кодирования (security parameter) последовательностей GUID, открытые параметры (public parameters) и главный закрытый ключ (master secret key):

$$S_G(P_S) \rightarrow (ID_{GU}, P_P, K_{MS}), \qquad (1)$$

где $S_G()$ — функция общей настройки системы, P_S — параметр стойкости протокола кодирования, ID_{GU} — GUID, P_P — открытые параметры, K_{MS} — главный закрытый ключ.

Открытые параметры, в свою очередь, могут быть определены через наборы атрибутивных общих ключей $K_{AP}(i,j)$ и атрибутивных закрытых ключей K_{AS}:

$$S_A(P_P) \rightarrow (\{K_{AP}(i,j)\}, \{K_{AS}(i,j)\}) \text{ где } i \in [1;I] \text{ и } j \in [1;J], \qquad (2)$$

где $S_A()$ — функция авторизации, параметр j соответствует атрибутивному центру, а параметр i — отдельному атрибуту.

Далее для каждого атрибута должна быть оуществлена генерация закрытого ключа S_K (который высылается далее пользователю) через функцию авторизации на базе GUID, главного закрытого ключа, открытых параметров и атрибутивных закрытых ключей:

$$G_{SK}(i, K_{MS}, P_P, \{K_{AS}(i,j)\}, ID_{GU}) \rightarrow S_K(i, ID_{GU}) \text{ где } i \in [1;I]. \qquad (3)$$

Кодирование текста осуществляется через функцию $E()$ на базе входного кода $\{D\}$, политику доступа P_A, набор ключевых слов S_{KW}, открытые параметры и наборы атрибутивных общих ключей. При этом сам закодированный текст $T_E()$ можно представить через функцию от входного файла T_D и индекс защиты закодированных данных I_E:

$$E(\{D\}, P_A, \{S_{KW}\}, P_P, \{K_{AP}(i,j)\}) \rightarrow T_E(T_D, I_E) \qquad (4)$$

Код доступа определяется функцией $TD()$ на базе параметров закрытого ключа, набора ключевых слов и открытых параметров

$$TD(P_P, S_{KW}, S_K(i, ID_{GU})) \rightarrow T_{KW}. \qquad (5)$$

Также следует определить ключ преобразования (transformation key) через закрытый ключ и значение z:

$$G_{TK}(S_K(i, ID_{GU}), z) \rightarrow T_K(ID_{GU}) \qquad (6)$$

Функция поиска базируется на T_{KW} и $T_E(T_D, I_E)$:

$$F_{Search}(T_{KW}, T_E(T_D, I_E)) = \begin{cases} 1, \\ 0, \end{cases} \qquad (7)$$

Если на выходе функции получается значение «1» — запрос выполнен успешно, и облачный сервер запускает алгоритм преобразования. Если значение на выходе соответствует «0» — алгоритм преобразования не будет запущен.

Построенная математическая модель предлагается в качестве методологической базы для разработки алгоритмов мультивариантного поиска по наборам ключевых слов и конфиденциальной передачи данных в средах IoT и IoE.

Выводы

Таким образом, в результате анализа особенности мультивариантного поиска в средах IoT и IoE была построена модель работы конфиденциальной передачи пользователем данных на ресурсы облачного сервиса. Показан приоритет в данной области атрибутивного кодирования, алгоритмов облегченного декодирования и мультиавторизации. На основе данного подхода была построена целостная методология разработки алгоритмов мультивариантного поиска по наборам ключевых слов. Анализ эффективности работы алгоритмов данного класса был оценен через релевантность результатов выполнения пользовательских запросов и нагрузку на вычислительную мощность аппаратного комплекса информационной системы.

Список литературы / References

1. *Long J., Zhang K., Wang X. & Dai H.-N.,* 2019. Lightweight Distributed Attribute Based Keyword Search System for Internet of Things. Security, Privacy, and Anonymity in Computation, Communication, and Storage Lecture Notes in Computer Science, 253–264. doi: 10.1007/978-3-030-24900-7_21.
2. Fuzzy identity and attribute based encryption for fine grained access control of encrypted data, 2018. International Journal of Modern Trends in Engineering & Research. 5 (7). 23–26. doi: 10.21884/ijmter.2018.5172.m7iz2.
3. *Qiuxin W.*,2014. A generic construction of ciphertext-policy attribute-based encryption supporting attribute revocation. China Communications, 11 (13), 93–100. doi: 10.1109/cc.2014.7022531.

4. A Survey on Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage. (2017). International Journal of Science and Research (IJSR), 6 (1), 1113–1116. doi: 10.21275/art20164283.
5. *Boneh D., Waters B.* Conjunctive, subset, and range queries on encrypted data. In: Vadhan, S.P. (ed.) TCC 2007. LNCS. Vol. 4392. Pp. 535–554. Springer, Heidelberg (2007).
6. *Zhenpeng L., Xianchao Z. & Shouhua Z.,* 2014. Multi-authority Attribute Based Encryption with Attribute Revocation. 2014 IEEE 17th International Conference on Computational Science and Engineering. doi: 10.1109/cse.2014.343.
7. *Cui J., Zhou H., Zhong H., Xu Y.* AKSER: attribute-based keyword search with efficient revocation in cloud computing. Inf. Sci.423, 343–352 (2018).
8. *Caro A. D. & Iovino V.,* 2011. jPBC: Java pairing based cryptography, 2011 IEEE Symposium on Computers and Communications (ISCC). doi: 10.1109/iscc.2011.5983948.
9. *Li Q., Feng D. & Zhang L.,* 2012. An attribute based encryption scheme with fine-grained attribute revocation, 2012 IEEE Global Communications Conference (GLOBECOM). doi: 10.1109/glocom.2012.6503225.
10. *Green M., Hohenberger S., Waters B. et al.* Outsourcing the decryption of ABE ciphertexts. In: USENIX Security Symposium. Vol. 2011, 2011.
11. *Hohenberger S., Waters B.* Online/offline attribute-based encryption. In: Krawczyk, H. (ed.) PKC 2014. LNCS. Vol. 8383. Pp. 293–310. Springer, Heidelberg, 2014.
12. *Liang K., Susilo W.* Searchable attribute-based mechanism with efficient data sharing for secure cloud storage. IEEE Trans. Inf. Forensics Secur. 10 (9), 1981–1992, 2015.https://doi.org/10.1109/TIFS.2015.2442215.
13. *Yang Y., Chen X., Chen H. & Du X.,* 2018. Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing. IEEE Access, 6, 18009–18021. doi: 10.1109/access.2018.2820182.
14. *Li H., Liu D., Jia K., Lin X.* Achieving authorized and ranked multi-keyword search over encrypted cloud data. In: 2015 IEEE International Conference on Communications (ICC), London, pp. 7450–7455. IEEE, June 2015.
15. *Li J., Zhang L.* Attribute-based keyword search and data access control in cloud. *In: 2014 Tenth International Conference on Computational Intelligence and Security*, Kunming, Yunnan, China, pp. 382–386. IEEE, November 2014.
16. *Li J., Yao W., Zhang Y., Qian H., Han J.* Flexible and fine-grained attribute-based data storage in cloud computing. IEEE Trans. Serv. Comput.10 (5). 785–796. September, 2017.
17. *Rajasekar M., Nisha S.P. & Thangarasu V.,* 2012. Scalable And Secure Sharing Of Personal Health Records Using Enhanced Attribute Based Encryption. Paripex - Indian Journal Of Research. 3 (2). 246–248. doi: 10.15373/22501991/feb2014/84.
18. *Miao Y., Ma J., Liu X., Li X., Jiang Q., Zhang J.* Attribute-based keyword search over hierarchical data in cloud computing. IEEE Trans. Serv. Comput. 5 (3) 1–14, 2017.
19. Fuzzy Identity And Attribute Based Encryption For Fine Grained Access Control Of Encrypted Data. (2018). International Journal of Modern Trends in Engineering & Research, 5 (7), 23–26. doi: 10.21884/ijmter.2018.5172.m7iz2.
20. *Ning J., Dong X., Cao Z., Wei L., Lin X.* White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes. IEEE Trans. Inf. Forensics Secur.10 (6), 1274–1288 (2015).
21. *Kumar V. & Madria S.,* 2015. Distributed Attribute Based Access Control of Aggregated Data in Sensor Clouds. 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS). doi: 10.1109/srds.2015.33.
22. *Wei J., Liu W., Hu X.* Secure and efficient attribute-based access control for multiauthority cloud storage. IEEE Syst. J.12 (2), 1731–1742 (2018).
23. *Zhang W., Lin Y., Xiao S., Wu J., Zhou S.* Privacy preserving ranked multi-keyword search for multiple data owners in cloud computing. IEEE Trans. Comput. 65 (5). 1566–1577, 2016.
24. *Rane D.D. & Ghorpade V.,* 2015. Multi-user multi-keyword privacy preserving ranked based search over encrypted cloud data. 2015 International Conference on Pervasive Computing (ICPC).
25. *Belguith S., Kaaniche N. & Russello G.,* 2018. Lightweight Attribute-based Encryption Supporting Access Policy Update for Cloud Assisted IoT. Proceedings of the 15th International Joint Conference on e-Business and Telecommunications. doi: 10.5220/0006854601350146.