Если n < 3m+1, то задача не имеет решения. Очевидно, что это довольно дорогое решение. Существует вариация Проблемы Византийских генералов, в которой используются подписанные сообщения. Это означает, что сообщения от верных генералов не могут быть подделаны или модифицированы. Для таких случаев существуют алгоритмы, позволяющие достичь консенсуса при условиях n ≥ m + 2.

Архитектура отказоустойчивых распределенных систем очень сложна. Существует множество различных проблем и ошибок, которые могут возникать в условиях распределенности и система должны уметь их обрабатывать. Корректно обрабатывать ошибки – наиболее сложная задача. На практике большинство ошибок вызваны проблемами с сетью, а византийские модели редко используются в силу своей сложности. Существуют готовые алгоритмы для решения проблемы консенсуса, однако они часто полагаются на различные допущения и поэтому не всегда могут быть использованы на практике без дополнительных модификаций.

Список использованных источников

1. Michael J. Fischer, Nancy A. Lynch and Michael S. Paterson, “Impossibility of Distributed Consensus with One Faulty Process,” Journal of the ACM, April 1985, 32(2):374-382. https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf
2. D. Dolev. "The Byzantine Generals Strike Again," Journal of Algorithms, 3, 1982, pp. 14-30.
3. L. Lamport. 1983. The Weak Byzantine Generals Problem. J. ACM 30, 3 (July 1983), 668-676. DOI=http://dx.doi.org/10.1145/2402.322398
4. Michael J. Fischer, Nancy A. Lynch, and Michael Merritt. 1985. Easy impossibility proofs for distributed consensus problems. In Proceedings of the fourth annual ACM symposium on Principles of distributed computing (PODC '85), Michael Malcolm and Ray Strong (Eds.). ACM, New York, NY, USA, 59-70. DOI=http://dx.doi.org/10.1145/323596.323602

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ КОГНИТИВНЫХ СЕРВИСОВ IBM WATSON, ДОСТУПНЫХ В РАМКАХ ОБЛАЧНОЙ ПЛАТФОРМЫ IBM BLUEMIX

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

Александр Александров, Виктор Козуб

Иван Пилецкий, канд. физ-мат. наук, доцент

IBM Watson представляет собой когнитивную систему, которая способна понимать, делать выводы и обучаться. Она также позволяет преобразовывать целые отрасли, различные направления науки и техники. Например, предсказывать появление эпидемий или возникновения очагов природных катастроф в различных регионах, вести мониторинг состояния атмосферы больших городов, оптимизировать бизнес-процессы, узнавать, какие товары будут в тренде в ближайшее время. Доступ к части сервисов IBM Watson доступен через использование API облачной платформы IBM Bluemix. О некоторых возможностях IBM Watson и пойдёт речь в данной работе.

IBM Watson — одна из первых когнитивных систем в мире. Эта система умеет очень многое, благодаря чему возможности Watson используются во многих сферах — от кулинарии до предсказания аварий в населенных пунктах. В общем-то, большинство возможностей Watson не являются чем-то уникальным, но в комплексе все эти возможности представляют собой весьма мощный инструмент для решения разнообразных вопросов. Например — распознавание естественного языка, динамическое обучение системы, построение и оценка гипотез [1]. Все это позволило IBM Watson научиться давать прямые корректные ответы (с высокой степенью достоверности) на вопросы оператора. При этом когнитивная система умеет использовать для работы большие массивы глобальных неструктурированных данных, Big Data. Получить доступ к возможностям Watson можно используя облачную платформу IBM Bluemix.

В США были проведены психологические исследования, которые подтвердили, что стиль письма человека, порядок слов, эмоциональный окрас напрямую связаны с чертами характера данного человека [2]. Предсказание к предрасположенности к определённым видам деятельности может быть сделано на основании анализа определённых черт характера данного человека. Результаты таких исследований напрямую легли в разработку алгоритмов когнитивных систем.

Одним из сервисов IBM Watson является сервис, позволяющий получить портрет личности человека, основываясь на лингвистическом анализе сообщений из соцсетей, электроной почты или любых других источников текста, который написал данный человек. Этот сервис носит название Personality Insights. Personality Insights базируется на психологии языка вкупе с алгоритмами обработки данных. Выходными данными данного сервиса является представление черт характера исследуемой личности в трёх моделях: модель Большой пятёрки (Big Five), модель потребностей (Needs) и модель ценностей (Values). В рамках данной работы мы исследовали возможности IBM Watson для применения в повседневной жизни. Одну из задач, которые мы попробовали решить, была задача выбора специальности для абитуриента, основываясь на портрете личности данного человека.

Для получения портрета личности, пользователь должен ввести текст о себе, либо предоставить свой

Twitter-ID. Текст должен быть написан непосредственно пользователем и иметь эмоциональный окрас. Например, пользователь в данном тексте может рассказать о себе, своей жизни, приятных моментах из детства либо своём взгляде на какую-либо проблему. Далее данный текст через API отправляется на обработку в IBM Watson, в ответ мы получаем портрет личности, представленный численно в трёх моделях. Полученные значения сверяются с эталонными для специальностей и в качестве ответа выбирается специальность, значения которой оказываются наиболее «близко» от значений пользователя. Самой большой проблемой является выбор этих самых эталонных значений для специальностей. В данный момент используются тексты с описанием специальностей, представленные на сайте университета и пропущенные также через Personality Insights. Выбор этих текстов нельзя назвать оптимальным. Наиболее лучшим вариантом был бы преданализ текстов выпускников данных специальностей, и не просто выпускников – а тех, что действительно осознанно сам выбрал эту специальность и считает, что он попал на учёбу в нужное место. Далее, проанализировав данные тексты, можно будет получить более точную оценку эталонных значений.

Нами было написано приложение, реализующее данный функционал с использованием когнитивных возможностей IBM Watson, развёрнутое на базе облачной платформы IBM Bluemix. Приложение было написано и успешно представлено на хакатоне IBM Bluemix Hackathon Moscow в 2015-м году, где вошло в тройку лучших проектов.

Список литературы:

1. IBM Watson. *What is Watson* [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.ibm.com/smarterplanet/us/en/ibmwatson/what-is-watson.html
2. IBM Watson Developer Cloud. *The science behind the Personality Insights service* [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.ibm.com/smarterplanet/us/en/ibmwatson/developercloud/doc/personality-insights/science.shtml

АНАЛИЗ ИСПОЛЬЗОВАНИЯ МЕТОДОВ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ДЛЯ ЗАЩИТЫ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ

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

Рогов М. Г.

Егорова Н. Г. – доцент, канд. техн. наук

Защита персональных данных – это целый комплекс мероприятий технического, организационного и организационно-технического характера, которые необходимы для защиты информации, относящейся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных) [1].

Проблема защиты данных с использованием криптографических преобразований имеет множество вариантов решения. Для осуществления безопасности имеющихся в наличии данных нужно соблюдать основные правила:

- обеспечивать конфиденциальность информации, передаваемой или хранимой в памяти;
- всегда подтверждать подлинность и целостность информации;
- при каждой установке соединения и входе пользователя в систему производить аутентификацию абонента.

Возможность осуществления какой-либо операции преобразования и изменения информации, которая выполняется одним либо несколькими пользователями системы, владеющими так называемым секретом, не зная которого нет возможности осуществить эту операцию, является основой всех криптографических преобразований информации [2].

Криптографические технологии аутентификации, шифрования и цифровой подписи используются для реализации указанных функций.

К криптографическим методам защиты в общем случае относятся:

- шифрование (дешифрование) информации;
- формирование и проверка цифровой подписи электронных документов.

Чтобы обеспечить конфиденциальность данных используются различные методы симметричного и ассиметричного шифрования, а также взаимная аутентификация на основе одноразовых и многоразовых паролей, смарт-карт, цифровых сертификатов и многого другого [3].

Современные криптографические системы и методы защиты информации должны обладать рядом общепринятых свойств:

- возможность расшифровать сообщение существует только при наличии;
- владение алгоритмом никоим образом не должно влиять на защищенность информации;
- без изменений остаются структурные элементы алгоритма шифрования;