
5G И IOT - ПРЕДИЗВИКАТЕЛСТВА, АРХИТЕКТУРА И ИНТЕГРИРАНЕ*

СУНАЙ А. АЛИЕВ, СТАНИМИР К. ЖЕЛЕЗОВ

5G AND IOT - CHALLENGES ARCHITECTURE AND INTEGRATION

SUNAY A. ALIEV, STANIMIR K. ZHELEZOV

ABSTRACT: *This article aims to provide reference points by which the integration of new communication standard 5g and growing interest and deployment of IoT from a number of leading IT companies in the field of computer information systems. The research visualize challenges architecture and integration of the two fields. Global use of a web adopted platforms is a new perception and different quality of use. Access to mobile internet becomes completely essential to carry out communication and activities of different types. Through the collaboration of 5g mobile standard and Internet of Things will create flexible work practices for everyone around the world. Growing mobile access to the Internet, cloud-based services, and big data analytics are allowing anyone, anywhere to leverage “big wisdom” – a whole new kind of globally connected & shared knowledge base.*

KEYWORDS: *5G, IoT, internet of things, mobile, communications, integration, challenges, architecture, integration, collaboration, systems, fields, flexible, access, landscape*

1. Въведение

Краят на XX век и началото на XXI век са белязани с редица фундаментални промени, свързани с развитието на информационните технологии, появата на Интернет и преминаването към икономики, базирани на знания. Свидетели сме на явления като дигиталната революция и глобализацията. Информацията става ключов ресурс за всяка една страна, била тя положителна или отрицателна. Използването и манипулирането ѝ са в известна степен начин на представяне на реалността от технологични устройства, която ни заобикаля. Устройства, които са част от нашето ежедневие, начин на поведение и разбиране. С темповете на развитие и комерсиализиране на иновациите е възможно хората сами по себе си да се превърнат не само в потребители на технологията, но и част от самата нея, т.е. посредници между устройствата и устройства сами по себе си – биологични компютри.

2. Същност на проблема

С навлизането на облачните услуги се откри възможност за разширяването на една нова индустрия, отново част от дигиталната революция – Интернет на нещата (IoT-Internet of Things). Концептуално тези две технологии са коренно различни. Разполагат с напълно различни парадигми и начини на имплементиране. Според [5, 6] неуспорим факт е, че водещи компании като Microsoft, Intel, Apple, Google, Huawei, Amazon и т.н. (табл. 1) инвестират изключително големи финансови ресурси в изграждането и функционирането на модел, който интегрира облачните услуги с интернет на нещата като провежда една двупосочна колаборация между тях. От своя страна е посочено в [7], че технологични гиганти като Qualcomm, Arm Holdings, AMD т.н. (табл. 2) също се борят за на пазара в отдела на микропроцесорите, които са ключът към управлението на устройствата от ново

* Настоящата статия е финансирана от Фонд „Научни изследвания” към Шуменския университет „Епископ Константин Преславски“ по проект № РД-08-119/2016 г.

поколение. В резултат на настъпващите промени се създава вазимосвързана екосистема на интернет на нещата, поддръжката на обекти, мрежи, сензори, микропроцесори, машини, концентратори на данни и програми с високо ниво на изкуствен интелект.

Таблица №1

Име на компания	Абревиатура	Отдел
AMAZON WEB SERVICES	AMZN	Интернет на нещата приложим към облачните услуги – платформени или софтуерни
AT&T	AT&T	Интернет на нещата приложим към мрежови компоненти и оборудване
AXEDA	XEDA	Интернет на нещата приложим към облачни услуги - базирани на софтуерни колекции и анализатори на данни, генерирани от сензори и други устройства
DELL	DELL	Интернет на нещата приложим към ентърпрайз технологии
GE	GE	Интернет на нещата приложим към софтуерна платформа, която интегрира машинно генерирани данни с традиционни и облачни бази данни
GOOGLE	GOOG	Интернет на нещата приложим към ежедневни дейности в реални среди – домашни, административни, корпоративни и производствени
HP	HP	Интернет на нещата приложим към изграждането на споделени връзки от по-високо ниво в рутер и суич устройства
IBM	IBM	Интернет на нещата приложим към M2M комуникации
INTEL	INTC	Интернет на нещата приложим към осигуряване сигурност на потребителя и данните, с които той оперира
MICROSOFT	MS	Интернет на нещата приложим към ежедневни бизнес дейности
FACEBOOK	FB	Интернет на нещата приложим към създаването на приложения от софтуерни компани
ORACLE	ORACLE	Интернет на нещата приложим към управлението на бази от данни
SAP	SAP	Интернет на нещата приложим към платформа за управление на мобилни приложения
QUALCOMM	QCOM	Интернет на нещата приложим към платформи с отворен код

Водещи производители на микропроцесорна техника за IoT устройства

Таблица №2

Производител	Абревиатура	Отдел
QUALCOMM	QCOM	Микропроцесорна техника за (IoT – интернет на нещата) устройства
ARM HOLDINGS	ARMH	Микропроцесорна техника за (IoT – интернет на нещата) устройства
INTEL	INTC	Микропроцесорна техника за (IoT – интернет на нещата) устройства
AMD	AMD	Микропроцесорна техника за (IoT – интернет на нещата) устройства
RED HAT	RHT	Микропроцесорна техника за (IoT – интернет на нещата) устройства
SIERRA WIRELESS	Swir	Микропроцесорна техника за (IoT – интернет на нещата) устройства
CISCO	CSCO	Микропроцесорна техника за (IoT – интернет на нещата) устройства
GOOGLE	GOOG	Микропроцесорна техника за (IoT – интернет на нещата) устройства
APPLE	APPL	Микропроцесорна техника за (IoT – интернет на нещата) устройства
IBM	IBM	Микропроцесорна техника за (IoT – интернет на нещата) устройства

Водещи производители на микропроцесорна техника за IoT устройства

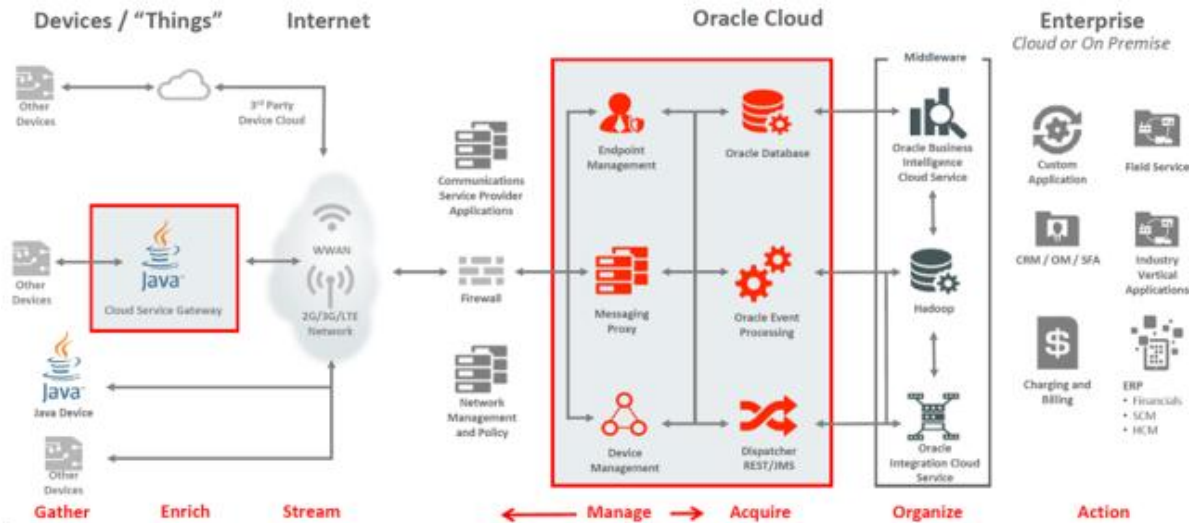
3. Теоритична постановка

След като облачните услуги вече са актуални и част от ежедневието ни, стана ясно, че е на лице необходимостта от сближаване им с интернет на нещата. Тази интеграция между двете технологии (фиг. 1), показва на информационното технологично общество единствено и само, че технологията е поема в правилната посока. Симбиозата между двете е необратима и е следващото стъпало към по-доброто потребление и използване на облачните услуги. В следствие на, което се стига до извода на това, че трябва този модел и парадигми да се съобразят и еволюират до етап на използване зелена енергия и енергия от възобновяеми източници. Причината за това е използването на голяма хетерогенна разпрделена сензорна мрежа, огромен брой сензорни потоци. Друг начин е да има паралелно използване на облачните услуги от интернет на нещата. Тези облачни структури могат значително да увеличат изчислителната мощност на продуктите базирани на модела – интернет на нещата и комуникацията между тях. Според [8] на (фиг. 2) може да се види до колко високо е заложен принципа на хибридность в зависимост от колаборацията между двете технологии.



Фигура 1

Облачните услуги реализират двупосочна връзка между няколко точки на комуникация: Анализ в реално време, Достъп до Облачна услуга и софтуерен програмен интерфейс. Три основни компонента комуникиращи си с дигиталните устройства и многокомпонентните обекти – образуващи интернет на нещата. За реализирането на подобрен комуникационен процес се изисква и висококачествена интернет скорост – 4G/LTE мрежа.



Фигура 2

4. Проблеми със сигурността

След разглежданите модели на интеграция и колаборация на двете технологии възниква може би най-важният въпрос – Какво е положението със сигурността в цялостния процес? В [5] се твърди, че с развитието на технолгията сигурността ще е ключов фактор в използването на интернет на нещата. Всички устройства ще бъдат уязвими сами по себе си от към злонамерени атаки. Атаки, които са проблем и при осигуряването на защитата в облачните услуги. Всички устройства разполагат с уникални идентификатори и могат да предават информация и данни по мрежата. Трафикът е активен non-stop. В следствие на което комуникацията идваща от облачните устройства и услуги е използван принципа M2M (машина-към-машина), интелигентните енергийни мрежи и автоматизацията им. В (табл. 3) от [1, 2, 3, 4, 5] се посочват основните видове облачни атаки, които са в сила и за устройствата от тип - интернет на нещата. Друг фактор са несигурните и не до там сложни потребителски пароли, които самите потребители задават при употребата на апликациите, които са обвързани с устройствата. Това ги прави лесни мишени за атака, извличане и манипулиране на лична, конфиденциална информация. По този начин достъпът и работата на приложенията се нарушава и устройствата могат да бъдат използвани по всички възможни начини с цел незаконни намерения.

Таблица 3

Име на атаката	Засегнати зони
DENIAL OF SERVICE	Хардуер IAAS, PAAS структури
CLOUD MALWARE INJECTION	Облачни инфраструктури
SIDE CHANNEL ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
AUTOTHENTICATION ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
MAN IN THE MIDDLE	Облачни инфраструктури, мрежови достъп и комуникация
AUDIO STEGANOGRAPHY	Облачни инфраструктури и мрежови комуникационен достъп
TARGETED SHARED MEMORY	IAAS, PAAS структури

PHISHING	Облачни инфраструктури, мрежови достъп и комуникация
BOTNETS	Облачни инфраструктури, мрежови достъп и комуникация
BACKDOOR CHANNEL ATTACK	Хардуер, IAAS, PAAS структури
FLOODING ATTACK	Облачни инфраструктури, мрежови достъп и комуникация
TRACEBACK	Облачни инфраструктури, мрежови достъп и комуникация
DATA STEALING PROBLEM	Облачни инфраструктури, мрежови достъп и комуникация
THEFT OF SERVICE	Облачни инфраструктури, мрежови достъп и комуникация
PORT SCANNING	Облачни инфраструктури, мрежови достъп и комуникация
ATTACK ON VIRTUALIZATION	Облачни инфраструктури, мрежови достъп и комуникация
STORAGE ALLOCATION AND MULTITENACY	Облачни инфраструктури, мрежови достъп и комуникация

От направеното проучване може да достигнем до следния извод. Интернет на нещата, изглежда, че може да бъде следващото голямо нещо в областта на технологиите. В [6] се посочва фактът, че сме в ерата на индустрия за един трилион долара, индустрия с милиарди долари от капиталови инвестиции се инвестират в нея. Мрежови устройства в дома, офиса, както и вградени в инфраструктурата и производството ще направят света по-ефективен и по-добро икономическо място. Както потребителите, така и производителите ще се възползват от по-голямата автоматизация, по-доброто събиране на информация и анализирането и, интуитивен потребителски интерфейс и дизайн. Кибер сигурност е фундаментът, който трябва да подсигури облачните услуги и интернет на нещата. Трябва да ги приоритизира като модели и подмодели. [9] Твърди, че е възможно е и таргетиране на уязвимите точки с цел предефиниране на приоритетите на сигурност, които действат сега в момента. Намесват се и фактори от рода на – коя операционна система използват нашите устройства, кои платформи и кои софтуерни услуги. Аспект, който малко потребители обмислят за важен. Ако производителят на съответната операционна система е допуснал грешки и оставил вратички образно казано за достъп и манипулиране на самата система и данните, които се съхраняват в нея – това я прави опасна за потребителя и за устройствата, с които тя си комуникира както и с облачните услуги, с които оперира. От своя страна пък това води до достъп и към останалите устройства, които са част от йерархията и структурата на облачните услуги и интернет на нещата.

5. Заключение

Докато този потенциал е на практика неограничен, има много притеснения около личния живот, сигурността и заплахата от хакери или злонамерени действия. И все пак, ако това е следващото голямо нещо, има редица компании, които инвеститорите могат да считат, освен за създатели на устройствата, но и за отговорни лица по пътя на имплементиране на сигурност и надеждност, при нормално потребление от страна на потребители. Те са крайната точка на действие и въздействие, и имат нужда от предоставена сигурност когато оперират с облачните услуги и интернет на нещата.

ЛИТЕРАТУРА

- [1] Khalil , I., Khreishah , A., Azeem, M. Cloud Computing Security: A Survey, Qatar Computing Research Institute (QCRI), Qatar Foundation, Doha, Qatar, ISSN 2073-431X www.mdpi.com/journal/computers
- [2] Singh, A., Shrivastava, Dr. M. Overview of Attacks on Cloud Computing, ISSN: 2277-3754 International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012
- [3] Siva, T., Krishna, E.S. P. Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5- May 2013
- [4] Zunnurhain, K., Vrbsky, V. Security Attacks and Solutions in Clouds, Department of Computer Science The University of Alabama Tuscaloosa, AL 35487-0290
- [5] <http://www.zacks.com/stock/news/213862/how-to-invest-in-the-internet-of-things> [онлайн, посетен 04.08.2016]
- [6] <http://www.computerworlduk.com/galleries/data/12-most-powerful-internet-of-things-companies-3521713/#13> [онлайн, посетен 04.08.2016]
- [7] <http://www.investopedia.com/articles/investing/010915/internet-things-2015.asp> [онлайн, посетен 04.08.2016]
- [8] <https://thecattlecrew.net/2015/12/06/introducing-the-oracle-iot-cloud-part-i-overview/> [онлайн, посетен 04.08.2016]
- [9] <http://www.computerweekly.com/feature/The-internet-of-things-is-set-to-change-security-priorities> [онлайн, посетен 04.08.2016]