THE INTERNET OF THINGS AND ITS APPLICATION IN VIRTUAL ECOSYSTEMS

Sunay A. Aliev, Plamen Ribarski

Email: sunay.aliev@yahoo.com; p_ribarski@abv.bg

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.*

ИНТЕРНЕТ НА НЕЩАТА И ПРИЛОЖЕНИЕТО МУ ВЪВ ВИРТУАЛНИТЕ ЕКОСИСТЕМИ

Сунай А. Алиев, Пламен Рибарски

Email: sunay.aliev@yahoo.com, p_ribarski@abv.bg

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.

Същност на проблема

[1] 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] неоспорим 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 и т.н.

(табл. 2) също се борят за на пазара в отдела на микропроцесорите, които са ключът към управлението на устройствата от ново поколение. В резултат на настъпващите промени се създава вазимосвързана екосистема на интернет на нещата, поддръжката на обекти, мрежи, сензори, микропроцесори, машини, концетратори 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 анализиратори 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 суитч 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

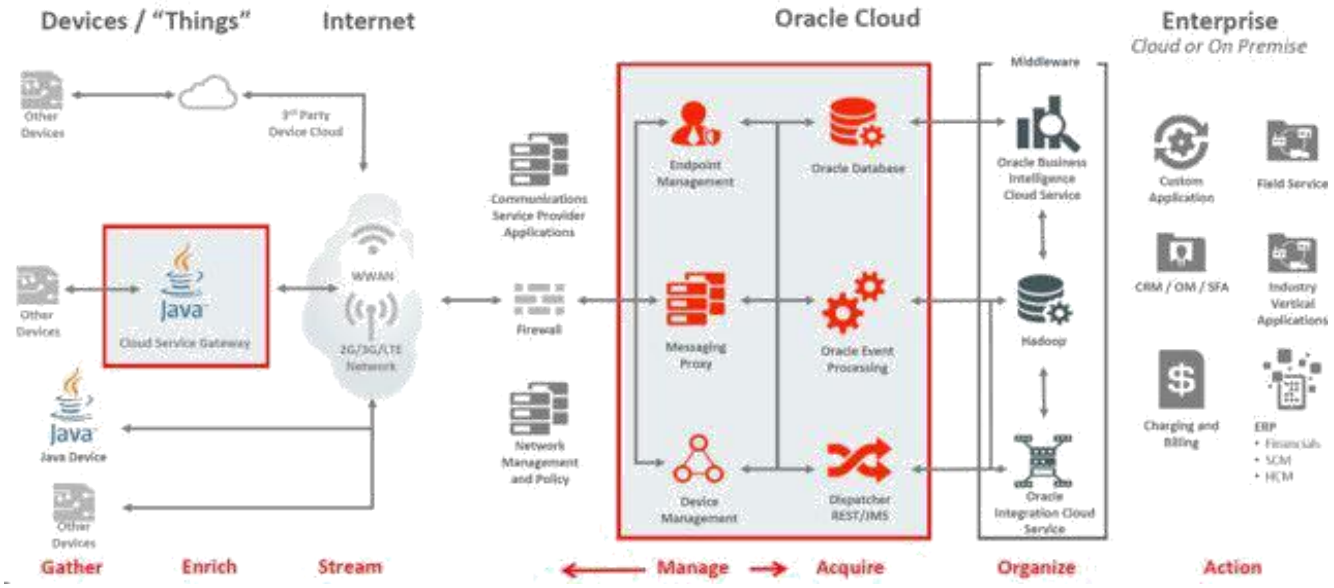
Производител	Абревиатура	Отдел
QUALCOMM	*QCOM*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
ARM HOLDINGS	*ARMH*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
INTEL	*INTC*	Микропроцесорна техника за (IoT – интернет на нещата) устройства
AMD	*AMD*	Микропроцесорна 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

Теоретична постановка

След като облачните услуги вече са актуални и част от ежедневието ни, стана ясно, че е налице необходимостта от сближаване им с интернет на нещата. Тази интеграция между двете технологии (фигура №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. Вследствие на което се стига до извода, че трябва този модел и парадигми да се съобразят и еволюират до етап на използване на зелена енергия и енергия от възобновяеми източници. Причината за това е използването на голяма хетерогенна разпределена 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 фигура №2 може да се види до колко високо е заложен принципът на хибридност в зависимост от колаборацията между двете технологии.

Фигура №1



Фигура №2

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 технологията 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 нон-стоп. В следствие на което комуникацията идваща от облачните устройства и услуги е използван принципът 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 устройства. 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 STORAGE ALLOCATION AND	Облачни инфраструктури, мрежови достъп и комуникация
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 икономически 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 уязвитите 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.

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 протребители. Те са крайната точка на действие и въздействие, и имат нужда от предоставена сигурност когато оперират с облачните услуги и интернет на нещата.

References:

1. Chappell, D. (August 2008). A short introduction to cloud platforms: An enterprise-oriented view.San Francisco, CA: Chappel and Associates.
2. Hutchinson, C., & Ward, J. (March/April 2009). Navigation the next-generation application architecture. IEEE ITPro, 18–22.
3. Borko Furht, A. E. (2010). Handbook of cloud computing. New York : Springer Science+Business Media.
4. Hemke M., Ubuntu Unleashed 2015 Edition: Covering 14.10 and 15.04, SAMS, Pearson Education.
5. Kanniga Devi and S. Sujan, ”A survey on application of cloudsim toolkit in cloud computing”,International journal of innovative research in science, engineering and technology, vol. 3, issue 6 pp. 13146-13153, June 2014
6. Cloud Standards Customer Council (н.д.). Извлечено от Cloud Standards Customer Counci: http://www.cloud-council.org/ (последно посетен на 09.10.2018)
7. Interoute. (н.д.). What is IaaS? Извлечено от Interoute:http://www.interoute.com/what-iaas (последно посетен на 18.10.2018)
8. Technopedia. (н.д.). Security as a Service (SecaaS or SaaS). Извлечено от Technopedia: https://www.techopedia.com/definition/26746/security-as-a service-secaas-saas(последно посетен на 15.10.2018)

Interoute. (н.д.). What is a Hybrid Cloud? Извлечено отInteroute: http://www.interoute.com/cloud-article/what-hybrid-cloud (последно посетен на 10.10.2018)