Д.О. Зуєв[1], А.В. Кропачов[2], О.Є. Усов[3], Д.М. Мостовщиков[4]
провідний архітектор мереж і хмарних обчислень, США[1]
керівник департаменту рішень автоматизації Bell Integrator USA[2]
ПАТ СК "Росгострах" Росія[3]
керівник відділу рішень системеої інсталяції Bell Integrator, Росія[4]

РОЗВИТОК МЕТОДІВ ХМАРНИХ ОБЧИСЛЕНЬ В РАМКАХ ПАРАДИГМИ «ІНТЕРНЕТУ ВСЬОГО»

Розглянуто тенденції розвитку хмарних сервісів в рамках парадигми «Інтернету Всього». Проведено аналіз взаємодії вузлів Інтернету Всього на рівнях машина-машина, людина-машина, людина-людина. Показані моделі надання послуг і особливості віртуалізації апаратно-програмних ресурсів хмарних сервісів. Розглянуто класифікацію кібер-загроз на прикладі життєвого циклу віртуальної машини як комплексу програмно-апаратних ресурсів хмарного сервісу. Запропоновано математичну модель визначення ефективності роботи нейромережі як частини інфраструктури хмарного сервісу. Розглянуто основні переваги туманних і росистих сервісів.

Ключові слова: *хмарні сервіси, автоматизація сервісу, віртуалізація інфраструктури, штучна нейронна мережа, туманні обчислення, росисті обчислення.*

Д.О. Зуев[1], А.В. Кропачев[2], А.Е. Усов[3], Д.Н. Мостовщиков[4]
независимый консультант, ведущий архитектор сетей и облачных вичислений, США[1]
руководитель департамента решений автоматизации Bell Integrator USA[2]
технический архитектор ПАО СК "Росгосстрах", Россия[3]
руководитель отдела решений системной инсталляции Bell Integrator, Россия[4]

РАЗВИТИЕ МЕТОДОВ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В РАМКАХ ПАРАДИГМЫ «ИНТЕРНЕТА ВСЕГО»

Рассмотрены тенденции развития облачных сервисов в рамках парадигмы «Интернета Всего». Проведен анализ взаимодействия узлов Интернета Всего на уровнях машина-машина, человек-машина, человек-человек. Показаны модели предоставления услуг и особенности виртуализации аппаратно-программных ресурсов облачных сервисов. Рассмотрена классификация кибер-угроз на примере жизненного цикла виртуальной машины как комплекса программно-аппаратных ресурсов облачного сервиса. Предложена математическая модель определения эффективности работы нейросети как части инфраструктуры облачного сервиса. Рассмотрены основные преимущества туманных и росистых сервисов.

Ключевые слова: *облачные сервисы, автоматизация сервиса, виртуализация инфраструктуры, искусственная нейронная сеть, туманные вычисления, росистые вычисления.*

D.O. Zuev[1], A.V. Kropachev[2], A.Ye. Usov[3], D.N. Mostovshchikov[4]
Independent Consultant Lead Arcitect, Network and Cloud, USA[1]
Bell Integrator USA Automation Solution Department Manager USA[2]
Technical Architect Russian Govt Insurance Russia[3]
Bell Integrator Russia, Moscow System Installation Solutions Department Manager[4]

DEVELOPMENT OF CLOUD COMPUTING METHODS WITHIN THE PARADIGM OF “INTERNET OF EVERYTHING”

The development trends of cloud services are considered within the paradigm of “Internet of Everything”. Interaction of three levels of Internet of Everything (machine-to-machine, person-to-machine, person-to-person) was discussed. Machine-to-machine communication type application was divided to services, people and environment sectors. Classification of cyber-attacks Run-Time Attacks, Start / Stop Attacks and Application Attacks based on stages of the virtual machine life cycle (creation, launch, working process, end and destruction) was proposed. Models of service providing and virtualization peculiarities of hardware and software resources of cloud services are demonstrated. A mathematical model for determining the efficiency of a neural network as part of the cloud service infrastructure is proposed. The main advantages of fog and dew services are considered.

Keywords: *cloud services, service automation, virtualization of infrastructure, artificial neural network, fog computing, dew computing.*

Introduction. "Internet of Everything" (IoE) is a modern paradigm of computer network which integrates all users, their devices, personal things, equipped with sensors, processes and data as nodes. This approach was most successful in establishing infrastructure, production lines and data centers of large corporations. But in recent years this trend has been spread to small-scale businesses and private users who actively use cloud services [1-3].

The IoE paradigm implies a newfound ubiquity of digital connectivity, which in general is divided into three levels (Fig. 1):

- machine-to-machine (M2M);

- person-to-machine (P2M);
- person-to-person (P2P).

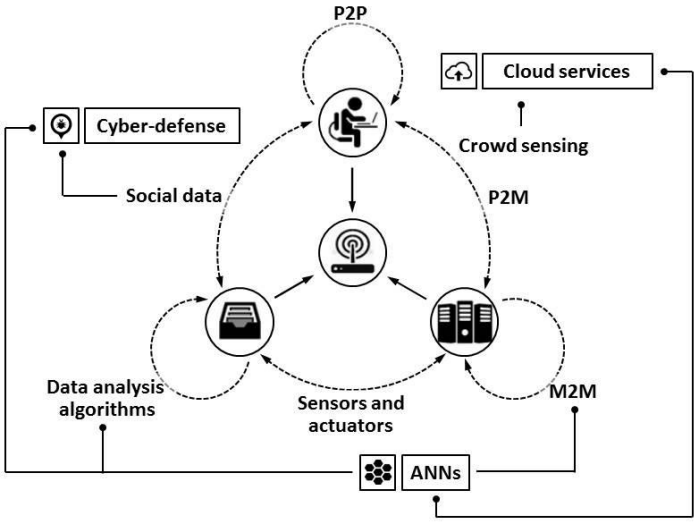

Fig.1. **Current trends in the development of the IoE paradigm**

Main trend of the IoE development is growth of the M2M communication type role and human resource management (HRM). Further spread of information technologies (IT) should not increase in the number of staff involved in supporting of network infrastructure but rather improve employee productivity.

M2M communication type application sectors are:

- Services: smart traffic monitoring; network infrastructure automation and defense; energy supply automation;
- People: healthcare monitoring; management in case of emergencies; maintenance of public order;
- Environment: the concept of "smart home"; logistics automation; the concept of "smart city".

Thus, M2M communication type not only significantly reduce number of P2M communication calls, which imply a specialization of employees and involve considerable labor costs, but also takes a part of the load for those P2P contacts that are associated with the analysis of the large groups of people interaction, where machine algorithms works better, excluding the so-called "human factor".

As it shown at fig.1 IoE paradigm trends could be linked with following IT-megatrends:

- implementations of processors, RAM, transmitters and sensors to household items;
- development of cloud services, including the virtualization of hardware and software resources
- implementation of fog and dew computing concepts;
- automation of the infrastructure of cloud services, including automation of hardware and software resources distribution and cyber protection;
- extensive adoption of artificial neural networks (ANNs).

In the framework of this work, it is proposed to consider modern approaches related to the virtualization of cloud storage resources, the use of fog and dew computing, and also to analyze the algorithms for the effective use of ANNs in the network services. The paper should comprise a good balance between theoretical part which summarizes the experience of cloud services and practical issues.

1. Virtualization of hardware and software resources of cloud services

Aspects of cloud computing hardware and software resources virtualization could be completely covered during analysis of typical cloud services (Fig. 2). Recently there are further cloud services types [3, 4]:

- Hardware as a Service (HaaS);
- Infrastructure as a service (IaaS);
- Platform as a service (PaaS);
- Software as a service (SaaS).

HaaS service model implies providing of user with equipment, which could be used to organize own infrastructure. In similar IaaS service model hardware resources are provided as the system evolves and user has control over the operating system (OS), as well as data storage and security policy protocols.

PaaS service model is based on the IaaS model but also includes an API programming interface. The user, therefore, has all tools to change the configuration of the hosting environment and software applications. In other hand, in the case of SaaS service model user accesses directly to the software resources of the cloud service. Therefore operability assurance, software updates and licenses obtaining remains on the provider side.

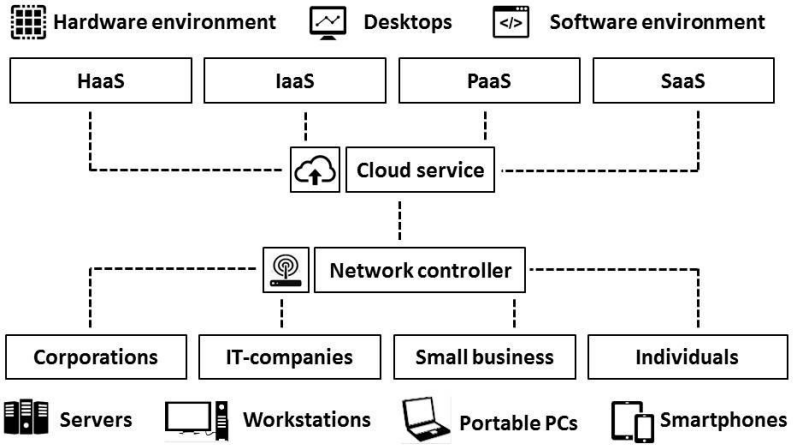

Fig. 2. **Basic algorithm of cloud services management**

All of the services mentioned above have their advantages and disadvantages depending on the area of use and working environment. For large corporations, it is important to have a possibility of infrastructure scaling and all network resources use, so HaaS and IaaS models would be preferred. At the same time, a lot of IT-companies cannot afford such a level of financial cost, so they choose PaaS as a compromise solution. For private entrepreneur and individual users time-based payment SaaS model will be sufficient.

Big cloud service providers often provide services at all possible levels. Let's analyze cloud services of transnational corporation "Google, Inc". "Google Cloud Storage" can be considered as IaaS model, "Google App Engine" is typical PaaS service, and the well-known applications "Gmail" and "Google Docs" are referred to SaaS model (Table 1). It should be noticed that servers and information storages that works in different models of services are not physically separated, since the separation of hardware and software resources is realized at the level of virtual machines (VM).

Table 1.

Cloud services management models

Cloud service provider	**Cloud services management model**		
	IaaS	**PaaS**	**SaaS**
IBM	IBM SmartCloud Enterprise	IBM SmartCloud Application Services	IBM LotusLive
Google Inc.	Google Cloud Storage	Google App Engine	Gmail, Google Docs
Amazon.com, Inc.	Amazon EC2	Amazon Web Services	AWS Mobile

VM should be considered as a hardware/software system that emulates a platform with the specified parameters to perform a certain tasks. VM construction is based on virtualization hardware and software resources provided to build an equivalent of a real environment for software algorithms implementation. During arrangment of the cloud service infrastructure work process, the service is considered as a complex of VMs, and every VM has its own security strategy and a security policy model. The security policy must contain a full set of possible types of data exchange, and thus any communication that goes beyond the security policy model is automatically considered as data transmission over a hidden channel, i.e. a data leakage channel or a cyber-attack channel. It should be noticed that the analysis of the classification of cyber-attacks on cloud storage as a VM complex differs

significantly from the classification of cyber threats for real network server, and this difference helps to understand the very mechanism of virtualization.

Classification of cyber-attacks on the VM complex methodology depends on life cycle analysis, i.e. period of VM existence and performing of the assigned tasks. After the project completion VM must be destroyed, which corresponds to the reorganization of the hardware and software resources of the cloud service.

There are further stages of the VM life cycle: VM creation, VM launch (start), working process, end of work (stop) and VM destruction. Thus there are three possible types of cyber-attacks: Run-Time Attacks (RTA), Start / Stop Attacks (SSA) and Application Attacks (AA). RTA-class of cyber-attacks is implemented before the VM creation and aimed at hardware environment and servers' OS of the VM complex. They use the hidden channels of the central processing units (CPU) and caches of real servers or some vulnerability of the OS. Obviously, this type of cyber-attack cannot be blocked by means of security policies to the VM. SSA cyber-attacks occur before the beginning of the VM work process or after the end of the VM work process. Usually they could be implemented by inserting of a code into the VM image right after VM creation or by copying sensitive data before its destruction. AA-class cyber-attacks intercept system queries or change the response code. This class of cyber-attacks is the most common one. The peculiarities of its implementation on cloud services are related to the fact that in this case it is necessary to analyze the vulnerabilities of the VM, rather than the real hardware and software complex, which gives more opportunities in the development of security strategies.

2. Application of artificial neural networks in cloud services. Recently application of ANNs in cloud services should be considered as a key mechanism to reduce the volume of P2M-communication and class of P2P-communications which are not related to social interaction on a personal level. The development of the IoE paradigm led to an exponential growth in the data that comes from each node of the system and should be analyzed in real time.

One can say that ANNs are used to recognition of images, which helps computer network to conduct an adequate analysis of the situation with minimal attendance of the support staff or completely independently. The procedures of image recognition includes recognition objects on a photograph, determining the nature of objects' interaction on a video, recognition of speech patterns and tracking intonation in an audio recording, recognition the cyber-attacks signatures which could be based on a known samples, etc.

Main advantage of ANNs is the principle of work process which is close to the principle of the human brain work. Thus, ANNs can replace a person in those areas where building of effective machine algorithms would be a nontrivial task [1, 5].

The basic elements ANN building (Fig. 3) are:

- selection of the ANN structure, first of all the organization of hidden layers and the hardware capabilities of the server environment;
- aggregation of database that contains a training samples;
- expert judgment that evaluates the ANN tutoring results and makes changes to the training samples database or the structure of the ANN.

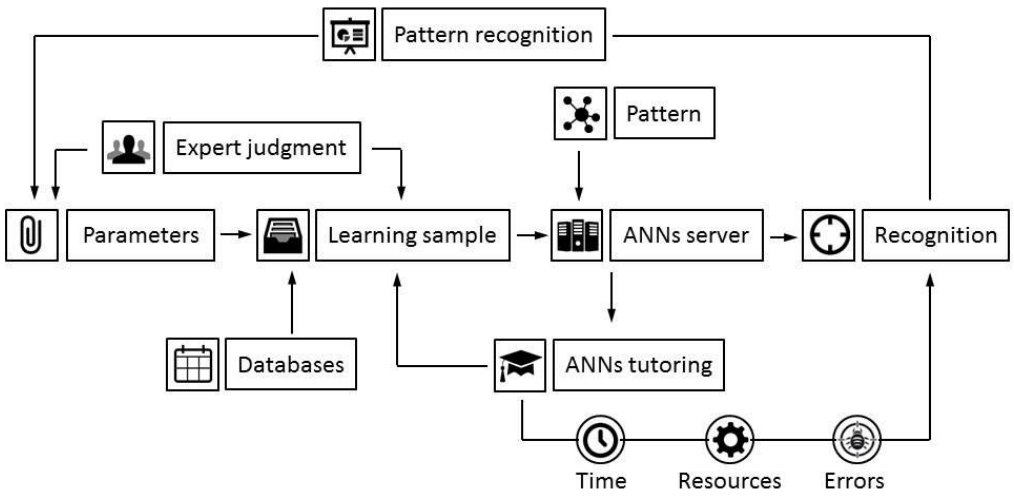

Fig. 3. Basic algorithm of ANNs tutoring and work

A systematic analysis of ANNs use in cloud services have shown that the key factors that characterize the efficiency of the network are following [1, 5]:

- the number of unrecognized images;
- number of falsely recognized images;
- adaptation of the ANN to the network service infrastructure;
- training samples database aggregation time;
- training time.

This list could be used to form concept of ANNs' use efficiency as a mathematical function, represented as:

$$E_{\Sigma} = f(E_{ANN}, E_{TS}), \tag{1}$$

where function E_{ANN} represents ANN efficiency and function E_{TS} represents efficiency of the training set. Those functions could be obtain by the following equations set:

$$\begin{cases} E_{ANN} = f(E_O, E_p, E_R) \\ E_{TS} = f = (E_F, E_A) \end{cases} \tag{2}$$

where E_O determines optimal structure of the ANN hidden layers, E_p — ANN parameters, E_R — ANN resource usage, E_F — efficiency of selection of the training sample features, E_A — efficiency of the training sample aggregation.

At the moment, for most practical problems, the class of suitable ANNs is already defined, which greatly simplifies the search for the optimal solution. The algorithm of the cloud service ANN work process can be demonstrated most clearly by the example of monitoring of cyber-attacks signatures in the framework of the cloud service security system, which is considered as a VM complex. As was shown above, cyber-threats are carried out through the transmission of data in hidden channel (TDHC). In the context of cloud service virtualization, the following three groups of TDHC can be considered:

- TDHC-1: the processes are performed within the same OS of one domain; the data is transferred from a more secure to a less secure level of the complex;
- TDHC-2: the processes are on different domains and, consequently, different platforms, and the data transfer is done through the network data storage or synchronization channels;
- TDHC-3: the channels are built within the VM OS, the transfer is carried out between different domains within the same platform.

To demonstrate the ANN work as a part of cyber-defense algorithms VM complex (Fig. 4), we will choose TDHC-3 cyber-attack group where hardware virtualization parameters analysis is an important part of are important security policies. At the physical level, the cyber-attack would be implemented through standard channels: CPU load, cache memory channel and networked shared storage.

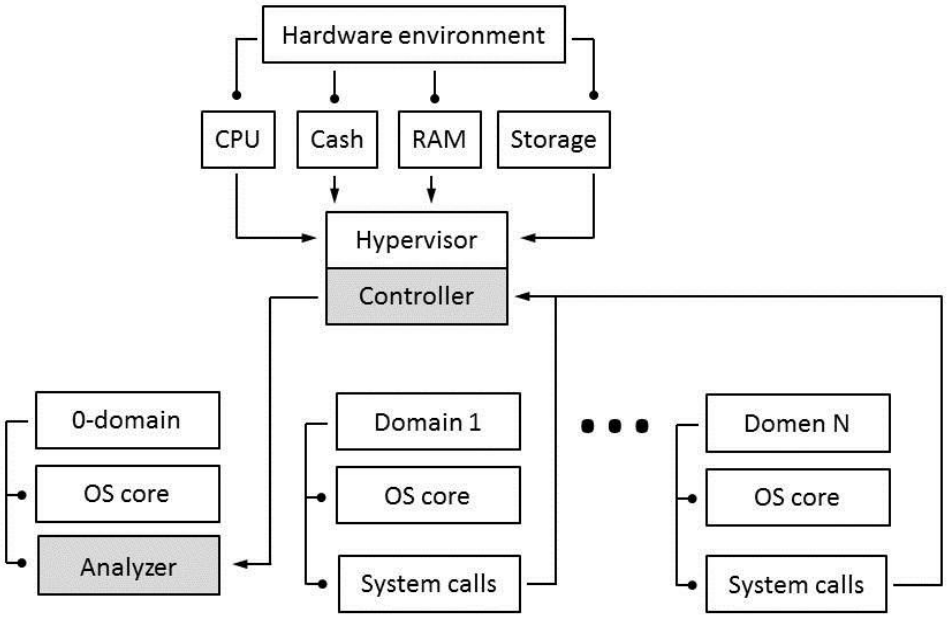

Fig. 4. **The algorithm of the cloud service ANN work process**

An effective algorithm for TDHC-3 tracking should meet following requirements:

- ultimate analysis of all available communication channels;
- 100% detection of cyber-attack signatures;
- tools for updating and scaling security algorithms;
- minimal VM platform resource usage;
- support of confidentiality regimes, policies and guidelines.

In the case of cloud services, the standard scheme of the cyber-defense system consists of an active controller (as part of the hypervisor) that intercepts the operations launched by the network's guests and the back-end server analyzer that is in the zero-domain and analyzes the intercepted operations to identify the TDHC (Fig. 4).

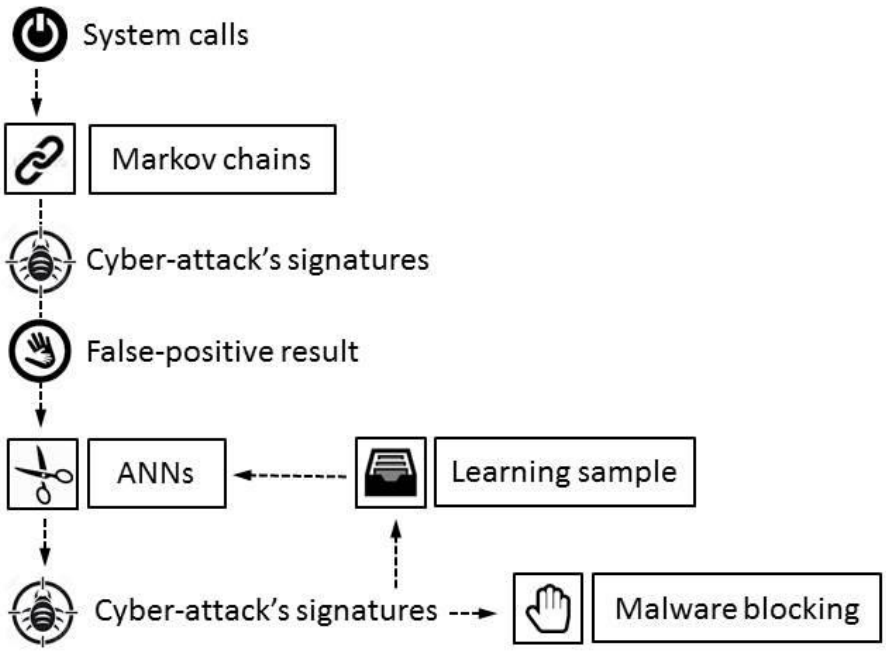

Fig. 5. **Analyzer of cloud service cyber-defense algorithm**

The hypervisor intercepts all signals that change state of the system and affect any processes within the cloud service infrastructure, so the controller is placed exactly in the hypervisor. In the framework of TDHC-3 group malware processes interact through common network resources in a hidden way. The detection algorithm should record all operations and changes in the system state, and even if the indications do not go beyond the limits defined by the security policy of the service VM, collected data should be transferred to the detector. The detector includes a detection module based on Markov chains, which in addition to determining the signatures of cyber-attacks gives a certain part of false positive results and a neural network detection module that separates false positive results from the cyber-attack signatures (Fig. 5).

3. Advantages of fog and dew computing within the "Internet of Everything". Development of the cloud computing concept is associated with the exponential growth of hardware capacities of computer hardware and network tools. Main trends in this area are:

- growth of the density of information recording (Fig. 6a);
- growth of the CPU frequency (Fig. 6b);
- growth of the network channel capacity (Fig. 6c).

Though, network channel capacity became a bottleneck of cloud services as part of IoE. Arrangement of all devices in a single network leads to most popular cloud services to the problem of request overstock which significantly affects the data transfer speed. Thus, "fog computing" was proposed. This concept implies redirection of user request to the least loaded and territorially close cloud service network (etymology of "fog computing" shows that "cloud" approaches to user and turns to the "fog"). This approach allows to significantly increase mobility of cloud computing and is suitable for working with data in use, while using classic cloud services is convenient to store large volumes of archival information and backup copies [6, 7]. However, within the framework of the fog computing

concept remains the problem of user dependence on the stable Internet channel. This problem is solved at the level of the concept of "dew computing" (Fig. 6d), which involves saving the most relevant data on the internal network drives of the user (similar to dewfall which indicates whether fog was likely to have occurred).

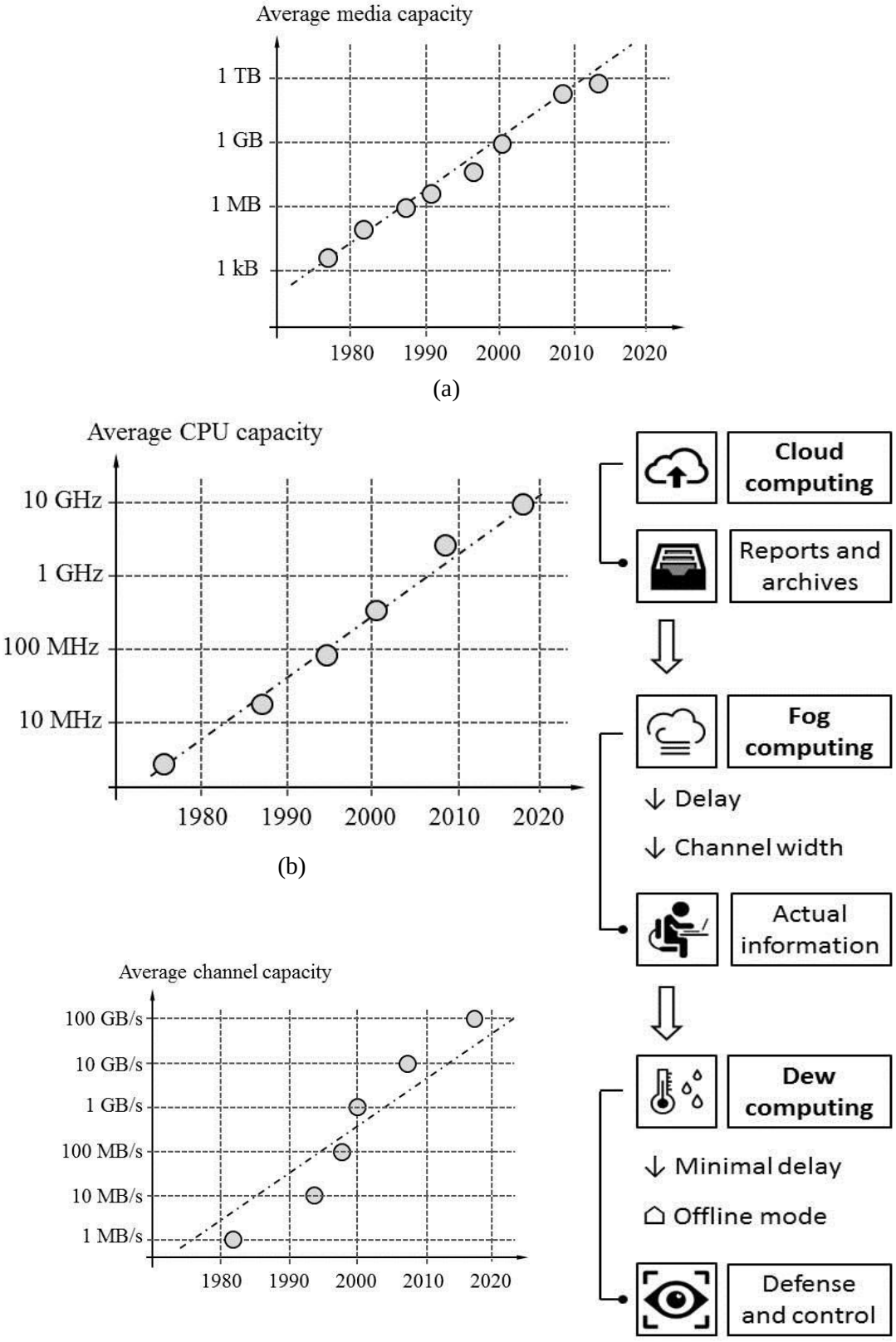

Fig. 6. **Development of the hardware capacities of the network services infrastructure (a, b, c) and the algorithm for the development of cloud computing to fog and dew computing (d)**

On the individuals' level, such an internal network can be considered FTP-servers of providers of housing estate, shopping and entertainment centers, multimedia servers of trains and excursion buses, as well as computers and smartphones of users. The concepts of fog and dew computing significantly improve cloud services and provide a high level of security.

The architecture of fog and dew services is similar to the architecture of standard cloud services, but certain parameters are more important. There are:

- security of the network infrastructure;
- confidentiality of data transmission;
- complete anonymity of resources;
- capabilities to scale the service.

These requirements are associated with an open and variable architecture of fog and dew services, most of which can be anonymous, which makes it impossible to pre-design the complex. Defense of system nodes should include the use of cryptographic methods for encrypting transmitted data, monitoring compliance with security policies that are carried out in real time, and the use of neural network methods to identify potentially dangerous code.

Conclusions. The development of cloud services are considered in the framework of the "Internet of Everything" paradigm. It is shown that the megatrends of the new paradigm are the virtualization of hardware and software resources, the development of the fog and dew computing concepts, the automation of the distribution of hardware resources and cyber-security of cloud services, and also adoption at network services of artificial neural networks. Models of providing services by cloud service providers are considered, in particular, HaaS, IaaS, PaaS and SaaS models. A mathematical simulation for determining the efficiency of a neural network as part of the cloud service infrastructure is proposed.

1. Manashty, A., & Thompson, J. L. (2017). Cloud Platforms for IoE Healthcare Context Awareness and Knowledge Sharing. Internet of Things Beyond the Internet of Things, 303.
2. Khaddar, M. A., & Boulmalf, M. (2017). Smartphone: The Ultimate IoT and IoE Device. Smartphones from an Applied Research Perspective. doi:10.5772/intechopen.69734.
3. Gordon, D. G. (2016). Legal Aspects of Cloud Computing. Encyclopedia of Cloud Computing, 462-475. doi:10.1002/9781118821930.ch38.
4. Appendix A: Example Of Microsoft Azure Cloud Service: Filemanager. (2016). Trustworthy Cloud Computing, 299-308. doi:10.1002/9781119114215.app1.
5. Security in the Cloud. (2017). CCSP® (ISC)2® Certified Cloud Security Professional Official Study Guide, 87-113. doi:10.1002/9781119419372.ch5.
6. Linthicum, D. S. (2017). Connecting Fog and Cloud Computing. IEEE Cloud Computing, 4(2), 18-20. doi:10.1109/mcc.2017.37.
7. Sojaat, Z., & Skalaa, K. (2017). The dawn of Dew: Dew Computing for advanced living environment. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). doi:10.23919/mipro.2017.7973447.

Стаття надійшла до редакції 23.02.2018