**Scientific and Practical Cyber Security Journal (SPCSJ) 4(3): 11-17 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)**

# SECURE CLOUD COMPUTING INFORMATION SYSTEM FOR CRITICAL APPLICATIONS

Sergiy Gnatyuk, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Vitaliy Kishchenko, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Andriy Tolbatov, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine
Yuliia Sotnichenko, NAU Cybersecurity R&D Lab
National Aviation University, Kyiv, Ukraine

**ABSTRACT:** The usage of cloud computing has gained a significant advantage due to the reduced cost of ownership of IT applications, extremely fast entry into the services market, as well as rapid increases in employee productivity. Everything can be implemented in the cloud service: from data storage to data analysis, applications of any scale or size. Employees also implement their own cloud applications for work, contributing to the development of their own cloud culture (BYOC). In addition, the use of cloud services is now available not only for large enterprises, but also for companies in medium and small businesses, which makes cloud technologies one of the main environments for the operation of their information systems. However, such an increase in the efficiency of working with cloud technologies has led to increased attention to the problems of cyber threats, the growth of which is inseperably linked with the growth of IT technologies. A cloud service user can deploy their own applications, build their infrastructure, or simply process data, but in any case, they trust their confidential data to the cloud service provider and want to be sure that their data is secure. Providing information security IS in a cloud environment is the responsibility of the provider, and therefore their systems must meet a number of requirements of both national and international law and international recommendations. Therefore, the main scientific and technical problem can be formulated as follows: data security may be compromised and there is a risk of mass data loss by many users due to the possibility of conducting cyber threats in cloud services. Because information is not only stored in the cloud, but is also processed, users must be confident in the security and availability of their data. The solution to this problem can be provided by using various methods of cyber threat detection, IDS / IPS systems, cyber incident response modules, etc.

**KEYWORDS***: information technology, cloud computing, security, critical applications, cyber attack.*

## INTRODUCTION

Cyber threat is any circumstance or event that may cause a breach of information security policy and / or damage to an automated system. The main purpose of cybersecurity is to prevent the implementation of existing cyber threats, ie to prevent the implementation of any cyber attacks, which are the sources of the following risks [1-4]:

– *Loss of intellectual property.* Analysis, conducted by the Skyhigh company, has found that more than 20 percent of the data stored in enterprises contains confidential information, including intellectual property. Most businesses now use multi-tier cloud services, where their data is stored on servers that are also used to provide similar services to other organizations. There are also several providers of cloud storage solutions that do not have modern data protection and security tools. Any security breaches encountered by the cloud service provider compromise confidential data.

– *Violation of compliance and regulations.* There are several regulatory requirements and compliance requirements for businesses in all markets and territories. This means that businesses have to make sure that their cloud storage and application providers take care of these regulations. Also, for businesses that promote the concept of Bring Your Own Device and Bring Your Own Cloud, make it difficult to comply with these standards. Any security breaches and data leaks can lead to severe penalties and loss of brand value.

– *Compromising credentials and authentication.* Poor certification and key management, weak passwords, and poor authentication are the causes of frequent data breaches in cloud applications: businesses struggle with authentication management issues because they reflect permissions and privileges for user roles; businesses very often do not delete or change user access when he / she resigns or changes role; the lack of multi-factor authentication is due to the compromise of 80 million customer records, and some cloud programs still do not have such authentication; Developers are often to blame for leaving cryptographic keys and credentials in the open source, making them free for analysis on portals such as GitHub.

– *API threats.* Most cloud solution providers offer their APIs for enterprise IT teams to help them with cloud services, management and monitoring. This makes the security and availability of cloud solutions dependent on the security of the API. Weak APIs expose cloud applications to the risks of accountability, confidentiality, integrity, and availability. For most businesses, such APIs remain the most vulnerable because they are fairly easily accessible directly through the Internet. Strict security-based intrusion testing and security checks are key elements in ensuring that these APIs are permanently protected from cyberattacks.

– *Hacking accounts.* Software exploits, phishing and fraud still are widespread occurrences. Cloud services are also susceptible to this kind of damaging cyber attacks, because cybercriminals have wider range of abilities to control user activities in public cloud services. In addition, there are two of the most effective measures for businesses cloud data and applications protection: to prevent users from accessing passwords and requisites of user accounts; ensure that multifactor authentication schemes are available where possible. Avoiding account data loss is the first step in protecting your cloud software from phishing and other breaches.

– *Improper usage of cloud services.* Cloud services can be misused, from using cloud resources to access encryption keys, to launch DDoS attacks on enterprise servers. The use of the enterprise's cloud resources for cybercrime has the following consequences: low availability of cloud systems; the impact of legal obligations in the form of lawsuits from influential parties; serious loss of reputation.

## REVIEW OF RELATED PAPERS

As mentioned earlier, cloud computing has considerable advantages over conventional “physical” computing [5-6]. However, this advantage - only for the direct user, because no matter what the user does - deploys its own infrastructure, launches applications, or simply stores and processes data – for him it will all be on remote servers, i.e. in the “cloud”. However, for a cloud computing service provider, the entire process from system construction to direct service delivery and maintenance takes place at the physical and hardware levels [7-9]. Therefore, problems at the software level include failures at the hardware level. The task is complicated when IoT (Internet of Things) tools are used in real production, and traditional approaches to cybersecurity cease to work effectively. Solving these problems will help to create conditions for a new corporate culture and technology for automatic protection of data, operations and applications [10-12]. It is an indisputable fact that the number and sophistication of cyberattacks is growing every year. According to a report by Alert Logic and Crowd Research Partners, more than half of security professionals in large companies predict the possibility of at least one cyberattack on their company. So it is not surprising that the business budget for these needs has grown by an average of 21%. The same report, based on a survey of 350,000 experts and experts around the world, says that today most attention is paid to the security of cloud infrastructure (33% of costs), cloud applications (28%), another 23% of costs go to increase staff qualifications.

The process of cyberattack prevention can be divided into two streams - descending and ascending. The first involves building a mechanism for classifying corporate data and add-ons by security and prescribing levels for each security protocol. The second is responsible for the use of tools and technologies to detect hacking attempts. Vulnerabilities are usually there. It can be taken for granted that the company is not able to protect itself from hacking the most "persistent" hackers. This means that all resources must be thrown to deter attacks until they cause irreparable damage to the data. In any situation, effective work with cyberattacks depends on proper planning. There should be

an effective method for instant identification of the source of the threat and a plan for its isolation, prevention of further spread [13-14].

**SECURE CLOUD COMPUTING INFORMATION SYSTEM**

Cloud environment in which the method of detecting cyber threats will be introduced.

The technology architecture is based on the recommendations of Cisco, which has developed its own progression of evolution of "cloud" data centers:

1) consolidation and aggregation of data center assets;

2) abstraction, is a key phase, because the assets of the data center are abstracted from the services that are actually supplied;

3) automation, which is capitalized on consolidated and virtual aspects, fast backup services and automatic modeling;

4) the interaction of the corporate “cloud” with the public;

5) the final phase - "inter-cloud", which replaces the existing types of "clouds".

Before building the architecture of the “cloud” data center, it is necessary to identify the system of components of the data center blocks in the basis of "cloud" architectures.

*10 Gigabit Ethernet.* The data center is designed with a high density of virtual machines that are combined with a large number of processors. From a network perspective, the growth of virtual machines and the concentration of cores will facilitate the transition to 10 Gigabit Ethernet as a necessary mechanism for providing servers. Specific benefits of the transition include: real-time policy configuration; mobile security and network policy, which is replaced by the policy of the virtual machine during its mobility; continuous operation of management models that establish management and operation of the environment for virtual machines and physical servers.

*Unified Fabric,* which gives all servers (physical or virtual) access to the local network, storage network, and IPC network, allowing them to be more integrated into the customer's network to increase efficiency and cost savings.

*Unified Computing.* The unified structure allows you to fully virtualize a "cloud" data center with pools of computer, network, and storage resources using unified computing. Unified Computing covers silos in a classic data center, allowing more efficient use of infrastructure in a fully virtualized environment, and creates a single architecture using standard technologies that ensure compatibility and investment protection. The Unified Computing system combines computing and network capacity, storage system access and virtualization resources in a scalable modular design that is managed as a single energy-saving system. This system can be managed using the built-in control system, in the Unified Computing platform.

In Fig. 1 shows the technological architecture, which presents the “cloud” data center of the next generation. The diagram shows examples of component blocks for the data center. In general, the completed architecture contains not only components of the structure, but also is regulated by different types of service and regulatory requirements.

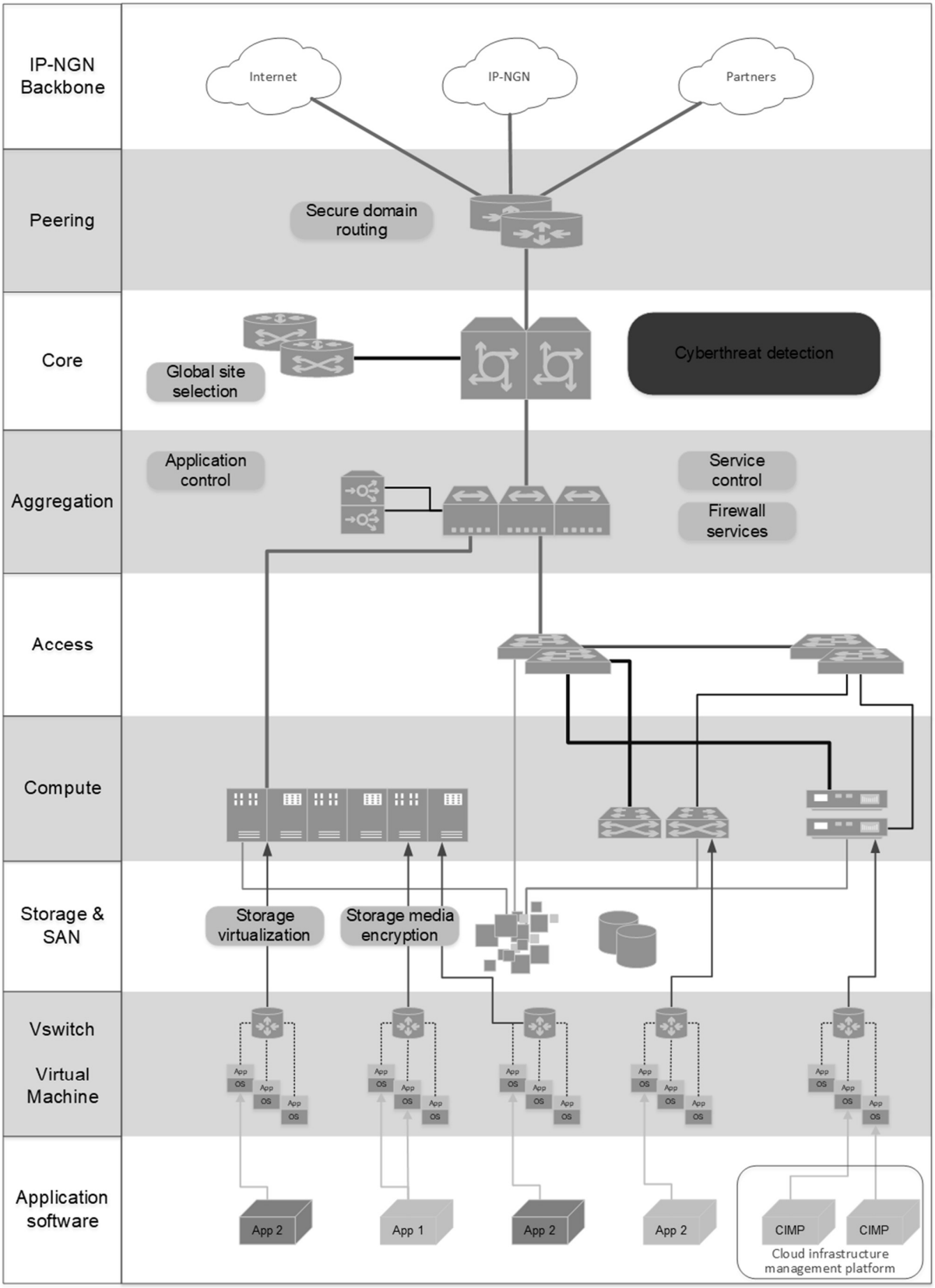


Fig. 1. Technological architecture of the data center based on Cloud Computing technology

The architectural model offers 9 tiers of the data center network:

- application software;
- virtual machine and distributed virtual switch (virtual machine, VSwitch);
- storage and storage networks (storage, SAN);
- calculation (compute);
- access;
- aggregation;
- core, where there is also a module for detecting cyber threats;
- peering;
- basics of the Internet (IP-NGN backbone).

Each subsequent level is connected to the previous one by a certain type of connection. From the application software tier to the Virtual machine & VSwitch tier, the App to HW / VM connection, then the virtual machine data, is fed to the distributed VSwitch virtual multilevel switches.

Data from the storage network (SAN) and application data from VSwitch are then transmitted to the computing tier using 4G FC (fiber chanel) and VSwitch to HW, respectively. The results of the calculations are sent to the access tier via 4G FC, 10G FCoE (Fiber Channel over Ethernet) and 1G Ethernet, and from this tier to the level of aggregation via 10G Ethernet. On this tier the control of applications and services is executed, and firewall services (IDS, SSL, anti-DDoS) are installed.

The next tier is the core, which also uses global location and cyber threat detection procedures. If a threat has been detected, the user and the system as a whole will be notified and appropriate action will be taken. At the peer-to-peer tier (the interconnection of individual networks to exchange traffic between users on each network), the domain is routed. The last tier is the Internet, using the 10G Ethernet connection type.

The downward movement of traffic and data occurs in the reverse order to that described above. Other key software components include: business applications for service tools; service management programs for service search, display and matching; SLA measurement, billing applications for reporting; web and business logic hosting applications. Key components of facilities: power supply and cooling of facilities; elements of the physical structure of data center components; racks and cable components.

Along with the technological component of the architecture of data centers, an important place is also occupied by the issue of trust in the infrastructure model of “cloud” computing. The key to gaining an advantage from the cloud is to establish a trust approach that begins with the establishment of such attributes in cloud architecture.

Trust in a "cloud" data center is based on several basic concepts:

1. Security: traditional data issues and resource access control, encryption and incident detection.

2. Control: the ability of the enterprise to directly manage the processes of deployment of applications.

3. Compliance and maintenance at the management level: compliance with general requirements.

4. Timely detection of cyber threats, prevention of intrusions, blocking cyberattacks.

Fig. 2 shows the structure of a protected data center based on Cloud Computing technology from the point of view of security, namely the models of threats and measures that need to be taken to minimize risks. The structure also reflects full control, compliance with requirements and agreements on the level of services.

The key idea of this model is that information security should not be secondary or simply part of the overall security, it should be disseminated and implemented at all levels of the architecture.

The threat profile (Threat profile) consists of such elements as:

- service disruption;
- data leakage;
- data disclosure;
- data modification;
- identity theft and fraud;

– intrusion.

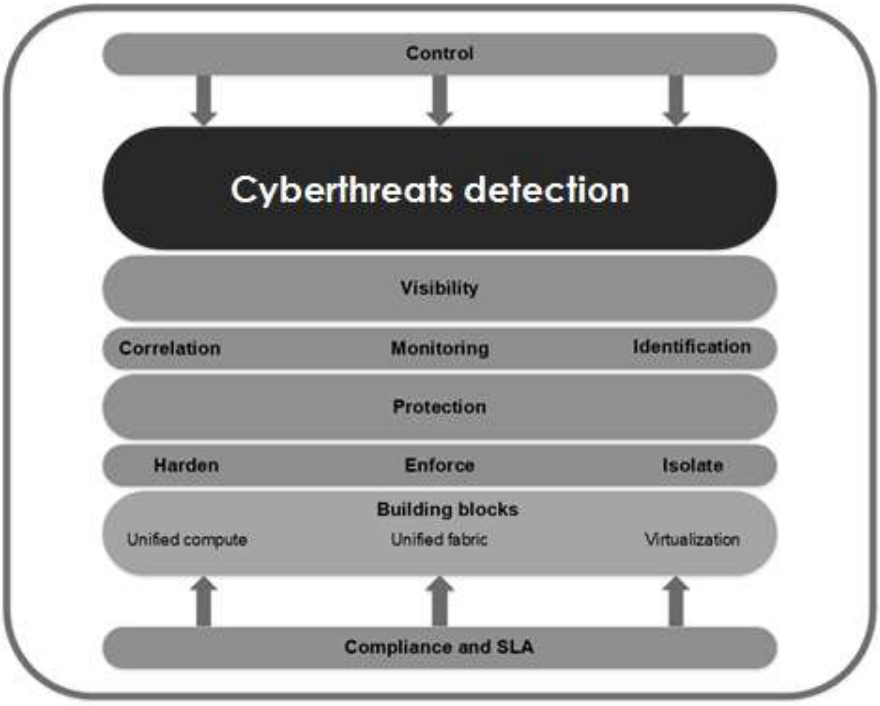


Fig. 2. The structure of a secure data center based on Cloud Computing technology

As can be seen from Fig. 2 detection of cyber threats is one of the most important tasks in the system of information security of cloud environments.

## CONCLUSIONS

In this paper the analysis of the existing models, systems and methods of detecting cyber threats was conducted, which allowed to identify their main shortcomings, namely: lack of data on experimental research, the impossibility of its use in cloud services (for the most part), some MVCs do not implement real-time cyber threat detection.

A model of cloud service has been developed, which through the use of technological architecture, high-speed communication, unified structures and calculations allows to ensure the security of cloud service based on Cloud Computing technology and conduct appropriate simulations.

## REFERENCES

1. R. Abidar, K. Moummadi, F. Moutaouakkil, H. Medromi, Intelligent and Pervasive Supervising Platform for Information System Security Based on Multi-Agent Systems, International review on computers and software. – 2015. – Vol. 10, Issue 1. – p. 44–51.

2. The 6 Major Cyber Security Risks to Cloud Computing [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://www.adotas.com/2017/08/the-6-major-cyber-security-risks-to-cloud-computing/

3. Google Security Whitepaper for Google Cloud Platform [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://habrahabr.ru/post/183168/

4. Data Mining for Network Intrusion Detection / P. Dokas, L. Ertoz, V.Kumarhttps // Recent Advances in Intrusion Detection. – 2014. – Vol. 15(78). – P. 21-30.

5. Ahmed P. An intrusion detection and prevention system in cloud computing:A systematic review / P. Ahmed // Journal of Network and Computer Applications. – 2016. – Vol. 11. – P. 1-18.

6. Anderson J.P. Computer Security Threat Monitoring and Surveillance / James P. Anderson // Technical Report Contract. – 1982. – Vol. 36. – P. 179-185.

7. Carl G, Kesidis G, Brooks RR, Rai S. Denial-of-service attack-detection techniques. Internet Computing, IEEE, 2006;10:82–9

8. How to build physical security into a data center [Електронний ресурс] / S.D. Scalet. – Режим доступу: World Wide Web. – URL: http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html?page=3

9. Al-Mamory S, Zhang H. New data mining technique to enhance IDS alarms quality. Journal in Computer Virology 2010;6:43–55

10. Breaking down what's in your cloud SLA [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: http://searchcloudcomputing.techtarget.com/essentialguide/Breaking-down-whats-in-your-cloud-SLA

11. ISO/IEC 27035:2011 – Information technology – Security techniques – Information security incident management, 2011. – 69 p.

12. Antonopoulos N. Cloud Computing: Principles, Systems and Applications / N. Antonopoulos // Springer Science Business Media. –2010. – Vol. 13(6). – P. 26-38.

13. Byrski A, Carvalho M. In: Bubak M, van Albada G, Dongarra J, Sloot P, editors. Agent-Based Immunological Intrusion Detection System for Mobile Ad-Hoc Networks Computational Science—ICCS 2008, 5103. Berlin/Heidelberg: Springer; 2008. p. 584–93.

14. AWS Global Infrastructure [Електронний ресурс]. – Режим доступу: World Wide Web. – URL: https://aws.amazon.com/about-aws/global-infrastructure/?nc1=h_ls