Developing a Model of Cloud Computing Protection System for the Internet of Things

Olexander Belej
Department of Computer-Aided Design
Lviv Polytechnic National University
Lviv, Ukraine
Oleksandr.I.Belei@lpnu.ua

Natalia Nestor
Department of Computer-Aided Design
Lviv Polytechnic National University
Lviv, Ukraine
natalia.nestor@gmail.com

Orest Polotai
Department of Information Security Management
Lviv State University of Life Safety
Lviv, Ukraine
orest.polotaj@gmail.com

Panchak Sofiia
Institute of Computer Science and Information Technologies
Lviv Polytechnic National University
Lviv, Ukraine
sofia.panchak@gmail.com

***Abstract*—This article proposes the use of a multi-agent approach when building a model of the cloud computing protection system of the Internet of things based on the reference architecture of cloud computing. It is proposed to build a system for monitoring user behavior in a cloud computing system using an automated model. The selection of a security agent is necessary on the one hand in connection with the increase in the number of commercial enterprises switching to the cloud computing platform, and on the other hand, with the need to protect data and resources on the Internet of things. The article also presents some scenarios for the interaction of actors based on a dedicated security agent. In this case, the security agent performs a controlling and connecting role between all the actors of the model, monitoring and recognizing unauthorized actions both by cloud users of the Internet of things networks and by actors of the cloud computing system of the Internet of things.**

Keywords—cloud protection system model, multi-agent approach, automata model, cloud computing, security agent, Internet of Things.

I. Introduction

Cloud technologies are very popular among active users of the Internet, as they provide a wide range of services in terms of multi-user structure, ease of operation, cost-effectiveness, and this, in turn, helps to improve the quality of user experience and entails the popularization of clouds in the Internet of things market. A very important aspect is the cost-effectiveness of cloud technologies, which is accessible to various segments of the population for storing information data. Some enterprises use public clouds instead of setting up their internal infrastructure for work that requires temporary computing, it is financially convenient, the calculation is only for the time of use. It must be remembered that the use of cloud technologies entails increased risks of information loss and, also, the possibility of control is limited. The study of the features of cloud computing from a position of information security can be structured as follows: data conservation from an uninterested party; the ability to manage and control the security issue, if necessary; real-time monitoring of violations; organization of the health of cloud services; addressing the issue of training qualified personnel in the direction of organizing the security of cloud systems; Regular investments in cloud security infrastructure development. If we consider the public cloud, then it, like many other systems that operate on the Internet, can be attacked. The following types of attacks are typical for cloud systems: standard attacks on software; attacks target the client; network attacks; attacks focused on cloud servers; implementation of diverse threats [1].

The development of modern information infrastructure is moving towards the creation of high-performance data centers (DC), application of virtualization technology and organization of cloud computing services (CS) based on it. The use of CS technology provides an increase in the efficiency of DC operation, however, it places high demands on the information security system and security features [2]. These requirements must take into account the dynamic nature of the use of information and computing resources, which in the CS environment are shared between users and services following the requirements of the information security policy (ISP) [3].

In the article [4] an assembly modeling for aircraft engines is used as examples to illustrate the system's effectiveness. The paper [5] proposes a new platform for using cloud computing capacities for provision and support of ubiquitous connectivity and real-time applications and services for smart cities' needs.

Other researching proposed Internet of Things system architecture offers a solution to the broad array of challenges researchers face in terms of general system security, network security, and application security [6]. In the Internet of Things vision, every physical object has a virtual component that can produce and consume services such as extreme interconnection will bring unprecedented convenience and economy, but it will also require novel approaches to ensure its safe and ethical use [7].

A new variant of RSA has been proposed called Memory Efficient Multi Key (MEMK) generation scheme [8]. In paper [9], considering such an IoT Cloud scenario, we present an architectural model and several use cases that allow different types of users to access IoT devices.

The security of stored data and information is one of the most crucial problems in cloud computing [10]. The paper [10] describes how to secure data and information in the cloud environment in time of data sharing or storing by using

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

our proposed cryptography and steganography technique. Industrial systems always prefer to reduce their operational expenses [11]. One such solution for industrial systems is a cyber-physical system (CPS) integration with the Internet of Things (IoT) utilizing cloud computing services.

The multi-agent approach is widely used in creating software tools for information systems that are responsible for solving some problems, starting with the issue of information retrieval and ending with the management and recognition of images [12, 13]. Research work in the field of using the multi-agent approach has been carried out for a long time, but the problem of constructing a universal model of a multi-agent cloud computing system has not yet been solved due to the complexity and diversity of the use of hardware and software platforms [14, 15]. This article proposes a model of a cloud computing system in the Internet of things networks with a dedicated security agent; it is necessary for monitoring the actions of a cloud user and system actors, as well as for ensuring the security of the system as a whole. A security agent is built using an automaton model.

II. The System Security Model of Cloud Computing Internet of Things

When building a model of a cloud computing system, it is necessary to take into account some system features:

- clients of cloud systems serve themselves, that is, they are allowed to independently gain access to information services;
- the universality of client access to the cloud system using information and telecommunication networks;
- the ability of the client to access information services using thin or thick clients through the information and telecommunication channel;
- high consolidation of computing resources - the combination of computing resources at one or more points for customer service with the ability to dynamically distribute physical and virtual resources following customer requests;
- dynamic scalability - the ability to quickly automatically change performance depending on the client's request [16].

A generalized model of a cloud computing system is presented in Fig. 1.

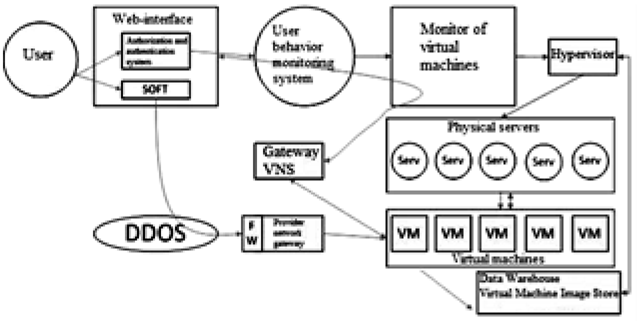

Fig. 1. Conceptual Model of the Internet of Things Cloud Protection System.

On the generalized model, you can see seven subjects: a virtualization system, a computing resources management system, a data warehouse, a virtual machine image repository, an authorization and authentication system, a web interface, and a user behavior monitoring system.

The virtualization system is a complete virtualization platform with the ability to use the hardware capabilities of the processor, most often hypervisors.

The computing resources management system is responsible for providing virtual machines to users through the management of a virtual monitor, as well as the allocation of various kinds of resources necessary for the user, in particular virtual networks, and virtual data storage.

The user behavior monitoring system is based on limiting and controlling user requests, as well as recommendations on fulfilling user requests in the cloud computing system, with the possibility of preventing unauthorized access to the elements of the cloud computing system, in particular, a virtual machine, hypervisor, data warehouse.

The model of interaction of subjects is shown in Fig. 2.

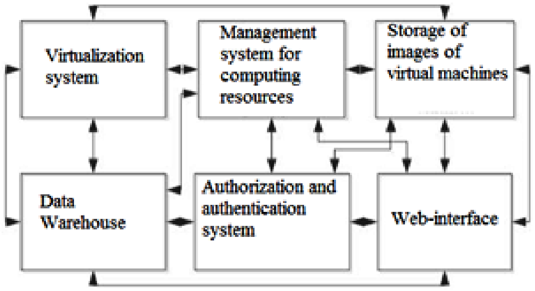
Virtualization system
Management system for computing resources
Storage of images of virtual machines
Data Warehouse
Authorization and authentication system
Web-interface

Fig. 2. A model of interaction of subjects in the protection system of cloud computing of the Internet of things.

The figure shows that the relationship in the model is organized by each one.

We have proposed a modernized architecture of cloud computing, it involves the use of 6 main acting actors (Table 1).

TABLE I. Actors of the IoT Cloud Computing

ACTOR	DEFINITION
User	A person or organization using cloud computing resources
Resource	The entity responsible for the availability of a cloud resource or service for the user
Auditor	A person or organization performing an independent assessment of the resources, services, maintenance of an information system, performance and security implementation of the cloud.
Broker	The entity controls the use and provision of resources and services to the user. Also establishing the relationship between the resource and the user
Telecommunications operator	Intermediary providing connection services between a resource and a user (communication channel)
Security agent	An entity that forms a request from a user to a resource, defines the processes necessary to provide a service or resource to a user and is responsible for the safe interaction of actors of the entire system as a whole

In this case, we use the actor model as the basis for modeling the cloud computing protection system. The idea of the composition of actor systems is an important aspect of modularity.

Based on a generalized model of a cloud computing system using a multi-agent approach, we construct a model for the interaction of acting actors in a cloud computing system.

The model of interaction of actors is presented in Fig. 3.

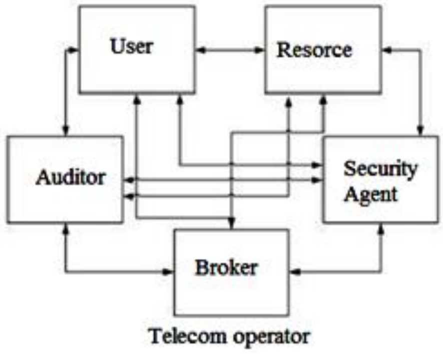

Fig. 3. A Model for Interaction of Actors in the Internet of Things Cloud Protection System.

We describe the possible scenarios of the interaction of actors, the additional security agent introduced by us is responsible for the integrity, confidentiality, and accessibility of the provision of resources and services, and also monitors the requests of system users and the interaction of system actors.

Scenario 1: A cloud user requests a service or service from a cloud broker instead of a direct request with a cloud resource. The user's request is generated in the security agent and sent to the cloud broker, who in turn creates a new service by combining a set of services, services, and resources. In this model, the cloud resource is not directly visible to the user, access is through a cloud broker (Fig. 4).

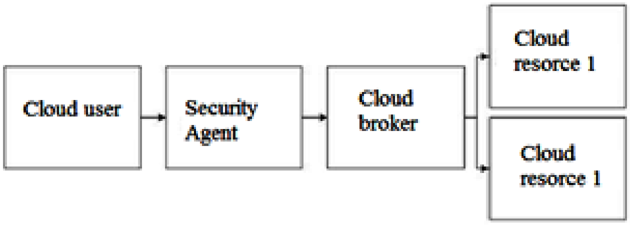

Fig. 4. The participation of a cloud broker in the interaction of a user and a resource in the system of protecting cloud computing of the Internet of things.

Scenario 2: A cloud service provider provides services for connecting cloud services from a cloud resource to a user (Fig. 5).

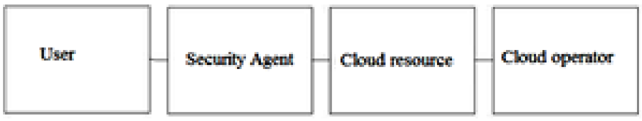

Fig. 5. The participation of the cloud carrier in the provision of resources and services in the Internet of Things cloud protection system.

Scenario 3: The cloud auditor conducts an independent assessment of the maintenance and security of the implementation of cloud services and services (Fig. 6).

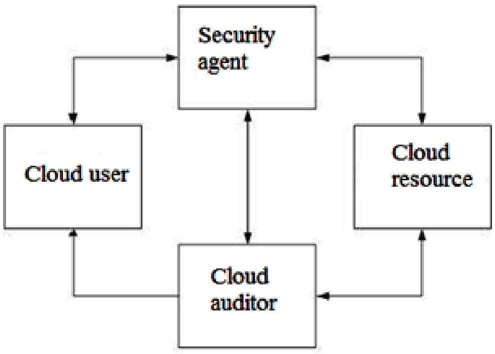

Fig. 6. The participation of the cloud auditor in the evaluation of the services provided in the protection system of cloud computing of the Internet of things.

We describe the functions and roles of actors in a cloud computing system. Cloud users are divided into three groups depending on the applications they require (Table 2).

TABLE II. IoT CLOUD COMPUTING USER ACTIVITY

User type	User activity	Users
Saas	A person or organization use applications or services to automate business processes	Business users
PaaS	Uses applications for the development, testing, and management of their projects deployed in the cloud	System administrators, project and application developers, people testing applications
Iaas	Monitor and create services and services for managing IT infrastructure	System administrators, system developers, and administrators, IT managers

A cloud resource is responsible for the availability of a cloud service or service for cloud users, solving problems in various service models (Table 3).

TABLE III. RESOURCE ACTIVITY IN THE INTERNET OF THINGS CLOUD PROTECTION SYSTEM

Resource type	Resource activity
Saas	Manages, installs, and maintains cloud-based application software
PaaS	Provides access to information technology platforms and tools for software development and administration
Iaas	Manages and provides computing resources and physical capacities of the system and networks, and also manages the cloud infrastructure

A cloud resource or service is seen as the deployment of services, service coordination, cloud service management, security and privacy (Fig. 7).

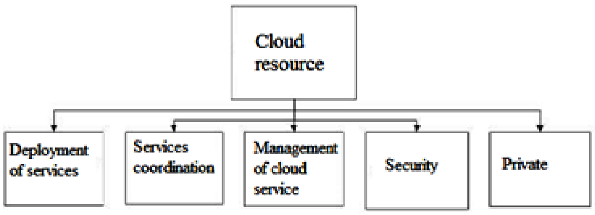

Fig. 7. Cloud Resource Blocks in the Internet of Things Cloud Protection System.

The main services provided by the broker are: expanding the cloud service, combining and ensuring the integration of cloud services, a selection of services for the user.

The cloud telecom operator is an intermediary providing connection service and access through network and telecommunication devices, and also provides delivery of services.

The security agent highlighted in Fig. 8, is responsible for generating a request from the user to the resource, also responsible for monitoring and adequacy of user requests in the cloud computing system, provides possible query options in case of incorrectly selected actions or attempts of unauthorized access to the resources of the cloud computing system, is also responsible for the interaction of actors in the system. This actor will be described in more detail below.

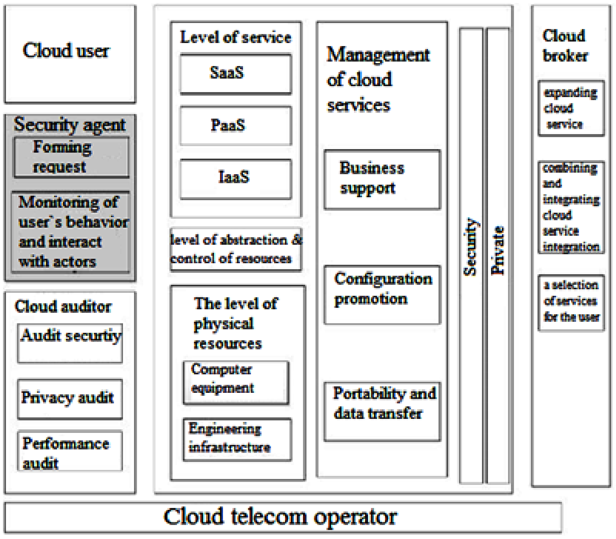
Cloud user
Security agent
Forming request
Monitoring of user`s behavior and interact with actors
Cloud auditor
Audit securtiy
Privacy audit
Performance audit
Level of service
SaaS
PaaS
IaaS
level of abstraction & control of resources
The level of physical resources
Computer equipment
Engineering infrastructure
Management of cloud services
Business support
Configuration promotion
Portability and data transfer
Security
Private
Cloud broker
expanding cloud service
combining and integrating cloud service integration
a selection of services for the user
Cloud telecom operator

Fig. 8. The conceptual structure of interaction of actors of the cloud system of the Internet of things.

The conceptual structure of the interaction of actors in the cloud computing system is presented in Fig. 8.

A security agent is an entity responsible for monitoring and the adequacy of user requests, for correctly sending a request to other actors in the system and for the interaction of actors. To understand the work of this actor, it is necessary to analyze user behavior in a cloud computing system.

III. The Security System Cloud Computing in the Internet of Things Networks

Security systems implemented within the framework of a multi-agent approach are justified to apply when the conditions for access to information resources are described using predicate relations or polynomials with free parameters. However, in the context of a dynamically changing configuration of information and network resources, the implementation of the requirements of mandatory, discretionary and role-based ISPs does not allow controlling such security aspects that are a result of the informational connectivity of subjects and objects of network interaction. These aspects are manifested when it is necessary to take into account: the conditions of situational awareness associated with the need for continuous updating of the state of subjects and objects of information interaction; ISP violation risks resulting from dynamic changes in the parameters and state of the VS; nonlocal nature of storage of peer-to-peer (P2P) and hybrid file-sharing networks information resources.

The CS environment is characterized by a dynamically changing set of computing resources - virtual machines, application containers, and software services managed by a large number of users. An important feature of the CS environment is that the resources are virtualized and share the hardware platform; they can be managed only remotely, over the network, without the possibility of direct physical access to them. The access control system in the CS environment should take into account the features of such systems, be able to reconfigure during operation - constantly update the ISP, request additional hardware at high load, and have a communication network for coordinated actions in a distributed CS environment.

In this case, the system component is a firewall, which, based on the information it has, decides on whether to allow or prohibit information interaction in the form of VS control. The solution to the protection problem should be implemented consistently, and the set of local solutions should be holistic from the ISP under consideration. The integrity property can also be considered from an emergent protection system; each firewall solves steps that do not ensure the full implementation of the ISP, but only a part of it, however, the totality of the decisions taken ensures the full implementation of the ISP and is an emergent characteristic.

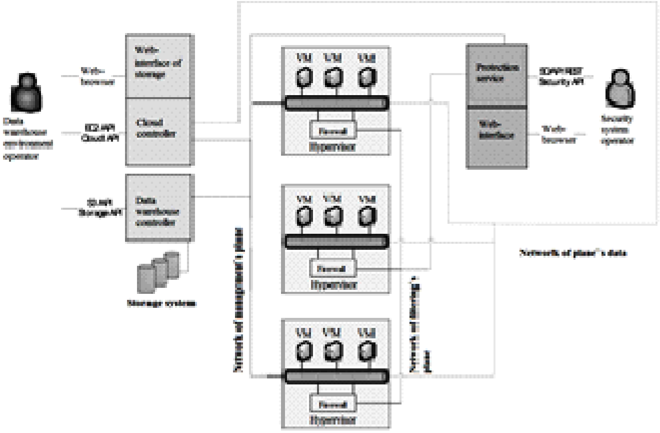

Fig. 9. Cloud computing system with an integrated security system in the Internet of things.

Figure 9 shows the high-level architecture of the access control system in the CS environment considered in the article. Information interaction is controlled by virtual machines (VMs) with firewalls software, which are run inside the CS hypervisors. Virtualized firewalls connect to the network subsystem of the hypervisor and filters VS between virtual resources and connections external to the hypervisor. Performance studies have shown that firewalls can be used effectively in a virtual environment. When using par virtualized drivers in the virtualized firewalls operating system, the performance drop is insignificant, about 10%, compared to the hardware-software solution.

IV. Discussion

The model for monitoring user behavior and the interaction of actors in the cloud system represents a signature model for searching for prohibited actions in the system. Our proposed algorithm for analyzing user behavior in a cloud computing system is designed to develop a security agent.

The proposed approach will increase the security of the system by increasing the reliability of recognition of unauthorized requests and user actions, as well as the interaction of actors in the cloud computing system.

A generalized model of user behavior and interaction of actors in the cloud system as a digital automaton A is presented in the expression by function (1).

$$A=\{S,S_o,X,Y,\delta,\lambda\}, \tag{1}$$

where *S* is the current technological state of the cloud computing system due to user actions, S_0 is the initial state of the cloud computing system, *X* is the input alphabet of user actions, *Y* is the output alphabet of reactions of the cloud computing system to user actions, $\delta(s, x)$ is the transition function cloud computing systems, $\lambda(s, x)$ is the output function of the cloud computing system.

So the figure shows a block diagram of the interaction of the cloud computing system and the subsystem for monitoring user behavior and actor interaction, according to which it controls all input and output values of the user, actors and the system as a whole, maintains a report on their work, affects the computer subsystem to implement the allowed transitions according to the table of exits and transitions (Fig. 10). The user performs an action on a computer subsystem under the influence of previous actions performed on it. The computer subsystem performs user actions only if the monitoring subsystem resolves. Control is carried out according to a pre-compiled table of exits and transitions.

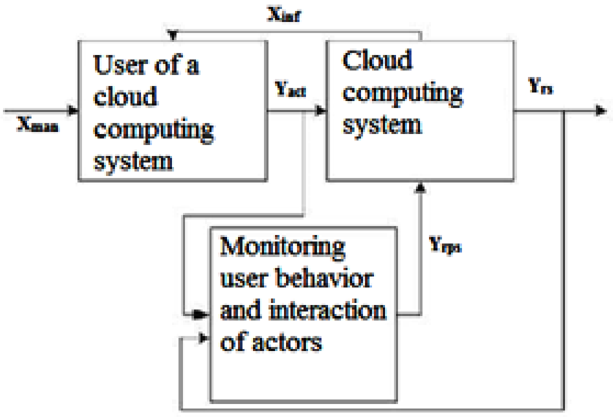
Xinf
User of a cloud computing system
Xman
Yact
Cloud computing system
Yrs
Monitoring user behavior and interaction of actors
Yrps

Fig. 10. The block diagram of the interaction of a cloud user and the Internet of things cloud computing system: X_{man} - the control effect on the user or actor, X_{inf} - the influence of the cloud system on the user or actor, *Yact* - the action of the user or actor on the cloud computing system, *Yrps* - a reaction of the subsystem of user or actor behavior to user actions, *Yrs* is the reaction of the cloud computing system to the action of the user or actor (the result of the cloud computing system).

The classification of user actions in the signature approach is shown in Fig. 11.

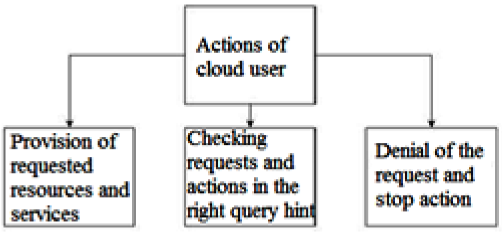
Actions of cloud user
Provision of requested resources and services
Checking requests and actions in the right query hint
Denial of the request and stop action

Fig. 11. Classification of user actions with a signature approach in the protection system of cloud computing of the Internet of things.

Depending on the type of user behavior and its actions, the cloud computing system adequately responds or suggests what needs to be done or blocks user actions. If the user requests resources without any deviations - the cloud computing system does not interfere (value *0*); if the user intentionally or not intentionally perform the prohibited action, the cloud computing system will block the user's actions and notify the administrator about the incident (value 1); in the case when the user does not make forbidden requests, but cannot perform the corresponding action, the cloud computing system prompts the user with subsequent requests that can be performed in the cloud computing system to obtain the desired result by the user (value *0,5*).

As a result of the analysis of the cloud computing system, the following information flows were identified: log-actions of the cloud auditor; log-actions of a cloud broker; log-actions of users of the cloud computing system; data about requests and actions of cloud computing users; information about the state of management objects. The graphic language for describing, modeling systems forms the basis of the IDEF0 approach and methodology.

The figure shows a model of information flows in the user behavior analysis system (Fig. 12).

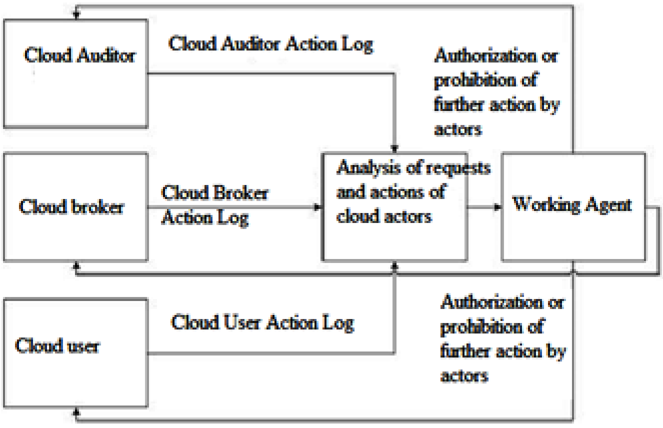
Cloud Auditor
Cloud Auditor Action Log
Authorization or prohibition of further action by actors
Cloud broker
Cloud Broker Action Log
Analysis of requests and actions of cloud actors
Working Agent
Cloud user
Cloud User Action Log
Authorization or prohibition of further action by actors

Fig. 12. Information flow model of cloud protection system in the Internet of Things.

For the developed tool, the main function is "Analysis of abnormal user behavior based on the automaton model". This will be the main block of the chart.

Next, you need to determine the input and output streams. Input streams are log-actions of the cloud auditor; log-actions of a cloud broker; log-actions of users of the cloud computing system; an algorithm for analyzing requests and actions of a cloud actor; patterns of normal and abnormal requests and actions.

Output streams are reports of requests and actions of actors; formation of patterns of requests and actions of actors.

The data approach for analyzing the anomalous behavior of users and actors in a cloud computing system based on an automaton model should be an element of this cloud computing system operating based on a virtual platform and will help to increase the level of security of the cloud computing system.

The main goal of a security system in a cloud computing system based on an automated model is to detect and block the main threats to information security in a cloud computing system.

The data approach should be universal and designed to protect the cloud computing system from both external and internal intruders; as well as for deciding on permission or prohibition of requests and actions of system actors; this requires an analysis of previous actions and requests of actors. During the functioning of the system, the database of signatures with allowing and prohibiting requests and actions is replenished, as well as the analysis and fixing of requests and actions in the cloud computing system.

V. CONCLUSION

The article presents the formalization of the protection system of cloud computing of the Internet of things. The model in the protection system of cloud computing of the Internet of things with a network-centric approach is generalized as a category that combines a class of objects and a transition between states. The IoT cloud protection system is implemented by managing VS bandwidth. A network-centric approach to organizing an access control system ensures the effectiveness of security features by checking in firewalls only those filtering rules that are necessary to protect cloud data between existing resources in the cloud, as well as the coordination of the functioning of all system components. Transparent integration of access controls is ensured by the ability of firewalls to function without the need to change the topology of the cloud network subsystem. At the same time, access control means remain invisible to participants in the information exchange.

We have defined mental properties for the actors of the cloud system of the Internet of things. A model for monitoring the behavior of a cloud user and the interaction of actors in this system is constructed, which is a signature-based search for prohibited actions in the system. A generalized model of user behavior and interaction of actors in a cloud system based on a digital machine is proposed. Information streams in the cloud computing systems are highlighted and a model of information flows is constructed, the IDEF0 context diagram.

In this regard, it becomes clear that the ideal solution to convince the client that his data will be safe is the compliance of the provided cloud services with the requirements of documents and standards to ensure the security of the data of the Internet of Things cloud protection system. Another option, providing the security of cloud services is the choice of information protection methods by cloud service providers from ready-made solutions already known on the market. Taking into account all the possible difficulties of using cloud systems in terms of data protection security, clouds have many times more advantages using Internet services and are becoming more and more popular in the modern market of information technologies, which is of interest to continuing research in this direction.

ACKNOWLEDGMENT

This work is carried out within the framework of the NAWA project nr. PPI/APM/2018/1/00031/U/001. The project is financed by the Polish National Agency for Academic Exchange.

REFERENCES

[1] X. M. Zhang and N. Zhang, "An Open, Secure and Flexible Platform Based on Internet of Things and Cloud Computing for Ambient Aiding Living and Telemedicine," 2011 International Conference on Computer and Management (CAMAN), Wuhan, 2011, pp. 1-4.

[2] W. He, G. Yan, and L. D. Xu, "Developing Vehicular Data Cloud Services in the IoT Environment," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1587-1595, May 2014.

[3] F. Tao, Y. Cheng, L. D. Xu, L. Zhang and B. H. Li, "CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System," in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1435-1442, May 2014.

[4] C. Wang, Z. Bi and L. D. Xu, "IoT and Cloud Computing in Automation of Assembly Modeling Systems," in IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1426-1434, May 2014.

[5] G. Suciu, A. Vulpe, S. Halunga, O. Fratu, G. Todoran, and V. Suciu, "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," in 19th International Conference on Control Systems and Computer Science, Bucharest, 2013, pp. 513-518.

[6] H. Ning, H. Liu, and L. T. Yang, "Cyberentity Security in the Internet of Things," in Computer, vol. 46, no. 4, pp. 46-53, April 2013

[7] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things," in *Computer*, vol. 44, no. 9, pp. 51-58, Sept. 2011

[8] C. Thirumalai and H. Kar, "Memory efficient multi-key (MEMK) generation scheme for secure transportation of sensitive data over cloud and IoT devices," Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, 2017, pp. 1-6.

[9] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, "An authentication model for IoT clouds," in IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), Paris, 2015, pp. 1032-1035.

[10] V. K. Pant, J. Prakash and A. Asthana, "Three-step data security model for cloud computing based on RSA and steganography," in International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 490-494.

[11] A. Sajid, H. Abbas and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," in IEEE Access, vol. 4, pp. 1375-1384, 2016.

[12] M. Al-Ayyoub, Y. Jararweh, M. Daraghmeh, “Multi-agent based dynamic resource provisioning and monitoring for cloud computing systems infrastructure,” in Cluster Comput, 18, 2015, p.p. 919–932.

[13] U. Siddiqui, G.A. Tahir, A.U. Rehman, Z. Ali, R.U. Rasool, P. Bloodsworth, “Elastic jade: dynamically scalable multi-agents using cloud resources,” in Second International Conference of the Cloud and Green Computing (CGC), 2012, pp. 167–172.

[14] S. Venticinque, L, Tasquier, B. Di Martino, “Agents based cloud computing interface for resource provisioning and management,” in Sixth International Conference of the Complex, Intelligent and Software Intensive Systems (CISIS), 2012, pp. 249–256.

[15] H. Huang, L. Wang, “P&p: a combined push-pull model for resource monitoring in a cloud computing environment,” in IEEE 3rd International Conference of the Cloud Computing (CLOUD), 2010, pp. 260–267.

[16] B. B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for Internet of Things & sensing-based applications," in Sixth International Conference on Sensing Technology (ICST), Kolkata, 2012, pp. 374-380.