INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2024, VOL. 70, NO. 2, PP. 413-420
Manuscript received September 13, 2023; revised June, 2024. doi: 10.24425/ijet.2024.149560

Cyber threats to the Private Academic Cloud

Valerii Lakhno, Bakhytzhan Akhmetov, Olena Kryvoruchko, Vitalyi Chubaievskyi, Alona Desiatko, Madina Bereke, and Maria Shalabaeva

***Abstract*—The potential breach of access to confidential content hosted in a university's Private Academic Cloud (PAC) underscores the need for developing new protection methods. This paper introduces a Threat Analyzer Software (TAS) and a predictive algorithm rooted in both an operational model and discrete threat recognition procedures (DTRPs). These tools aid in identifying the functional layers that attackers could exploit to embed malware in guest operating systems (OS) and the PAC hypervisor. The solutions proposed herein play a crucial role in ensuring countermeasures against malware introduction into the PAC. Various hypervisor components are viewed as potential threat sources to the PAC's information security (IS). Such threats may manifest through the distribution of malware or the initiation of processes that compromise the PAC's security. The demonstrated counter-threat method, which is founded on the operational model and discrete threat recognition procedures, facilitates the use of mechanisms within the HIPV to quickly identify cyber attacks on the PAC, especially those employing "rootkit" technologies. This prompt identification empowers defenders to take swift and appropriate actions to safeguard the PAC.**

***Keywords*—information security; private academic cloud; cyber threats**

I. Introduction

THE educational framework within higher education institutions, such as large universities, is comprised of various subsystems. Central to these subsystems is the unified Information and Educational Environment (IEE) of the university. The primary objective of the university's IEE is to facilitate the learning process for students and to offer the informational services that support this process. The era where educational resources functioned autonomously is gradually becoming obsolete. Such autonomous resources are now being superseded by cloud technologies and computing. These advancements are not only prevalent in education but also play a pivotal role in inter-university scientific collaborations [1]. From an Information Security (IS) viewpoint, cloud computing possesses distinct characteristics [2]. One notable aspect is determined by the fact that clients, such as universities that incorporate cloud technologies, do not have direct access to the vendor's cloud infrastructure. As a consequence, these remote cloud services remain outside the direct control of the client. The virtualization of computing systems, combined with the use of the Internet for accessing cloud technologies, broadens the scope of IS challenges at the physical and network tiers of the university's Cloud-Oriented Learning Environment (COLE). Concurrently, it becomes imperative to address issues concerning adherence to consumer standards, particularly in data storage.

A defining trait of the cloud computing environment within universities is the dynamic interplay between subjects and objects of information interaction. Developers of software and hardware tools for information protection each have distinct perspectives on the mechanisms of Information Security (IS) provision. As a result, the information protection market typically showcases products targeting well-known vulnerabilities. However, the development of advanced IS mechanisms for the cloud computing environment in educational settings isn't just about guarding against known vulnerabilities. It also involves anticipating and preventing novel, unrecognized attack methods (such as those employing "rootkit" technologies). Moreover, there's a focus on formulating new threat models and devising strategies to prevent or counteract cyberattacks on information assets housed within universities' private academic clouds.

All of the above predetermined the topic of our research.

II. Literature review

For modern educational institutions, including universities, ensuring Information Security (IS) has become a paramount concern. However, the creation of a protection system goes beyond merely designing information protection mechanisms. It's a continuous and multi-faceted process, intertwined with the perpetual exploration of new ways to bolster the IS of universities, especially as emerging technologies like cloud computing become integrated into the educational landscape. This sustained focus on IS is necessitated by the escalating number of cyber threats, which hold the potential to inflict significant harm upon educational institutions.

In [2] and [3], the authors address the issue of effective security management for cloud applications. However, their focus leans towards a general perspective of cloud computing IS, rather than diving into specific technical nuances of the issue.

In [4], the overarching concepts of virtual private cloud security are explored. The author delves into the fundamental aspects of private cloud operations and underscores the importance of private cloud IS frameworks.

Valerii Lakhno is with National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine (e-mail: lva964@nubip.edu.ua)

Bakhytzhan Akhmetov and Madina Bereke are with Abai Kazakh National Pedagogical University, Almaty, Kazakhstan (e-mail: bakhytzhan.akhmetov54@mail.ru, madina13.04@mail.ru)

Olena Kryvoruchko, Vitalyi Chubaievskyi and Alona Desiatko are with State University of Trade and Economics, Kyiv, Ukraine (e-mail: {kryvoruchko_ev, chubaievsyi_vi, desyatko} @knute.edu.ua)

Maria Shalabayeva is with Kazakh University Ways of Communications, Almaty, Kazakhstan (e-mail: m.shalabaeva@mail.ru)

In [5], the discussion revolves around threats, challenges, strategies, and solutions concerning cloud computing IS, particularly in a corporate structure. The authors sift through survey data, shedding light on cloud structure IS and examining favored cloud computing architectural models from an IS assurance standpoint.

In [6], [7], and [8], comprehensive studies on the IS of IaaS model components are presented. The authors pinpoint vulnerabilities inherent to the IaaS model and advocate for tailored countermeasures. Specifically, in [6], a security model tailored for IaaS is introduced, aiming to streamline the IS assessment process and enhance the security posture of the IaaS model.

In [9], a cloud-based static analysis system is presented, designed to detect security vulnerabilities in PHP. The system, as conceived by the authors, aids users in discerning elements that influence source code vulnerabilities within cloud settings.

In [10], the authors are pioneers in highlighting IS challenges within the cloud framework of educational institutions. They accentuate the prevalent cloud security vulnerabilities in educational settings and elucidate the methodologies employed to navigate these intricacies.

In [11], the focus is on obstacles hindering cloud computing adoption within universities and colleges in the Philippines. The discussion, inter alia, touches upon facets of cloud computing IS in an educational context.

In [12], a strategy to mitigate risk factors associated with utilizing cloud computing in education is proposed. However, the scope of this solution is restricted solely to enhancing login security.

According to the authors of the study [13], the responsibility of maintaining a high level of IS lies with the end users of the cloud-based academic structure. However, the authors do not at all address the issues of hidden threats in a private academic cloud.

In [14], [15] the authors discuss the IS issues of academic users of the cloud environment as well as the technical issues that affect the IS of the academic cloud.

In [16], [17], [18], [20], [21], [22], [23] the authors consider the tasks of countering cyber threats in the cloud environment. The focus is on the operational identification of potential vulnerabilities at the levels of access control processes to applied information services of guest operating systems. The tasks of control at the level of system calls of hypervisors are also touched upon. As the authors' research has shown, the complexity of solving these problems is related to the dynamism of changing states of the cloud environment. This feature can be used by attackers to organize attacks on hypervisor subsystems, which are responsible for scheduling tasks in the cloud and verification of commands for compliance with IS requirements.

Given the above, the task of countering cyber threats in the cloud infrastructure of educational institutions and, in particular, universities, is relevant. Our research is devoted to the solution of this problem.

III. THE PURPOSE AND OBJECTIVES OF THE STUDY.

The research aims to develop a cyber threat recognition method for a university's private academic cloud.

Research objectives:

1) *Development of an algorithm for the predicative identification of cyber threats for a Private Academic Cloud University based on the application of the basis of operations model and discrete threat recognition procedures (DTRP);*
2) *2. Implementation and testing of the software "Threat Analyzer".*

IV. METHODS AND MODELS

During the research, taking into account the peculiarities of the subject, were used: Boolean algebra and fuzzy set theory; methods and means of simulation.

Let one examine the components of the hypervisor (hereafter denoted as HIPV) as potential sources of cyber threats (CT) during attacks by those who violate security policies (SP). These attackers may then distribute, for instance, malware on the virtualization servers of the university's Private Academic Cloud (PAC), as illustrated in Fig. 1.

Attackers can target the components of the HIPV, as depicted in Figure 1. Such attacks involve sending deceptive processing requests to the HIPV's software modules, leveraging undocumented features of system and application software. This type of software is typically found on virtualization servers. The execution logic of all such programs is monitored from a potential denial-of-service perspective. This oversight heightens the risk of concealed threats to the PAC. Furthermore, these threats compromise not just the functional capabilities, but also the overall Information Security (IS) of the university's PAC.

Covert threats can result in potential disruptions to the PAC's operations. For instance, these threats might manifest through the actions of malware. At the guest OS level, there isn't any protection against such threats. In the context of our study, realizing these covert threats means harnessing mechanisms to synthesize and alter the context for implementing flows within the PAC. Through these flows, data can be transferred from entities with a high level of Information Security (IS) to those with a lower IS level, circumventing established rules. Consequently, the health and security assessment metrics of the HIPV can be compromised. The primary functions of the hypervisor include isolating different operating systems from one another and managing VM and guest OS resources. In the HIPV, as in any OS, several entities are created - EUM^*.

By entity (EUM^*) we mean - (Sub, O) with different level of IS. The operation of entity spawning $Create(Sub_i, O_m) \rightarrow Sub_j$ is commonly referred to as spawning with the control that the object has not been changed.

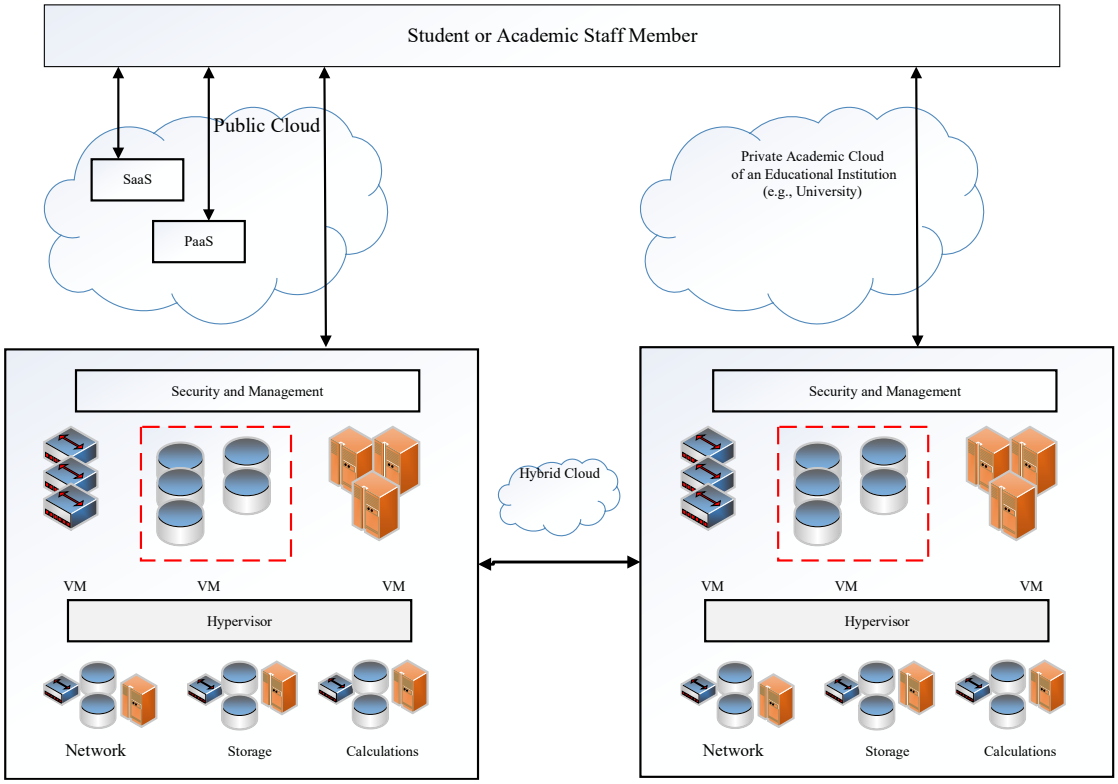

Fig. 1. Scheme of deployment of virtual workplaces in the University's COLE

This is true for any point in time $t > t_0$. That is, at this moment the operation $Create$ is activated. Creation of objects of the type Sub_j will be possible only if the source object is identical with respect to the moment t_0. That is, the following relation is true:

$$O_m[t] = O_m[t_o], \quad (1)$$

where $O, Sub -$ objects and subjects of access respectively.

In the case of using PAC as an element of the university COLE, objects and subjects can change roles. Therefore, in order to counteract the hidden threats in the university COLE, it is necessary that at the moment t_0 there are only flows from any Sub to any O_m that do not contradict the correctness conditions. This statement is true for PAC, in which there are generation rules with invariance Sub control O. For example, a security monitor must implement special mechanisms to identify the context of the monitored streams. This is true for both subject and object access in a PAC. And both Sub (initializing access) must use only permitted access mechanisms.

To this end, it has been proposed to introduce a set that is suitable for creating both access objects (O) and when spawned O as the following tuple [15]:

$$\langle s, Ord, Con\_type \rangle, \quad (2)$$

where $Con\_type -$ is the type of context of the monitored data flows in the PAC; $s -$ the increase or decrease of privileges for PAC users; $Ord -$ the type of process.

The creation of a new access subject Sub_j is possible only if:

$$O_m[t] = O_m[t_o],$$

where $j, m -$ are the numbers of objects in the presented specification of the PAC.

Monitoring is implemented in relation to operations that generate new objects. If necessary, e.g., when scaling up the PAC, we extend the monitoring to detect disguised cyber threats to the PAC or to the COLE as a whole. By the predicative function of identifying disguised (or hidden threats), we mean the representation of the eight-level model of operations shown in Fig. 2. Operations are considered with respect to a set of possible states in accordance with [15], [16]. The scale of states is adopted as follows: dangerous, safe and uncertain. In this case, the masked threat model is described in the form of the following tuple:

$$M = \langle Sourses, Servises, Devices, proc, Actions, hv, vm, Sec\_Roles \rangle, \quad (3)$$

where $Sourses -$ access subjects or processes, threat sources; $Servises -$ a set of SP rule templates. Adopted rules that are commonly used by traditional information protection systems; $Devices -$ devices that can be installed on the virtualization servers of a PAC. Meaning devices that are used by VM guest OSes; $proc -$ a set of impact subjects. Such subjects include

hypervisor malware, virtualization tools, etc.); $Actions$ – (actions) execution of operations by the subject. Only those operations that pose a threat to the access subject are considered; hv – the interaction environment of the processes of a set of VMs in the HyperV; vm – a set of VMs; Sec_Roles – procedures for multilevel role-based SP of the PAC.

In the framework of the proposed approach, the threat model for the PAC is considered as a system of interaction of HIPVs, see Fig. 2. It is assumed that there are eight levels of hierarchy: $S1$ – application levels; $S2$ – guest OS kernel levels; $S3$ – interrupt handler levels; $S4$ – HIPV memory manager levels; $S5$ – HIPV I/O subsystem levels; $S6$ – HIPV task scheduler levels; $S7$ – HIPV hardware managers; $S8$ – HIPV executive region levels of processors or processor cores. The levels $S1 - S5$ are where traditional information protection systems operate. These information protection systems use SP template sets to control access to the PAC. At the $S6 - S7$ malware levels, disguised threats are realized, which are discussed in [16], [17], [18]. The level $S8$ monitors the execution of VM operations taking into account the SP requirements [15], [17].

On the basis of the methods of combinatorial analysis in relation to possible transitions (if events from the set E) occur, it should be proved that if the number of levels of the hierarchy is equal to eight, the reflections correspond to the expression $S_i \times E_i :\to S_j$. If the number of levels is less than eight, the reflections are not isomorphic. Each transition will correspond to a collection of initialized predicates. The number of all possible substitutions of predicates into the function for evaluating the admissible states of the PAC will be $n!$

The block diagram for the predicate process identification method for defense against disguised cyber threats in a PAC, is shown in Figure 3.

In the proposed solution, the HIPV components in a PAC are described as a finite automaton:

$$Mod_i = (E_i, R_i, Start, \Pr_i, F_i, P_i, V_i), \quad (2)$$

where Mod_i – is the set of components of the environment of interactions of VM processes; F_i – the transition function of HIPV between states under external influences V_i; $\Pr_i$ – the privilege levels in a state R_i; P_i – the state admissibility functions. Or a tuple of predicates $\langle s, Ord, Con\_type \rangle$.

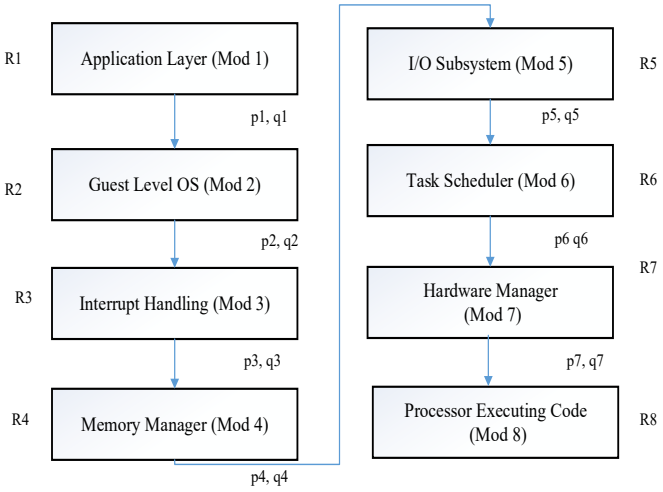

Fig. 2. A flowchart describing the interaction of VM processes in a private academic cloud HIPV

Predicates must meet the following conditions: $s = 0$ *if* $Max(\Pr_i, \Pr_j)$ – increase privilege level; $s = 1$ *if* $Min(\Pr_i, \Pr_j)$ – decrease privilege level; $Ord = 0$ – parent process; $Con\_type = 1$ – read/write operations for applications; $Con\_type = -1$ – read/write operations for VM guest OS; $Con\_type = 0$ – transaction pending.

The start of the algorithm corresponds to the startup of the VM. This is followed by a list of VM user requests, which are represented by a certain set of operations.

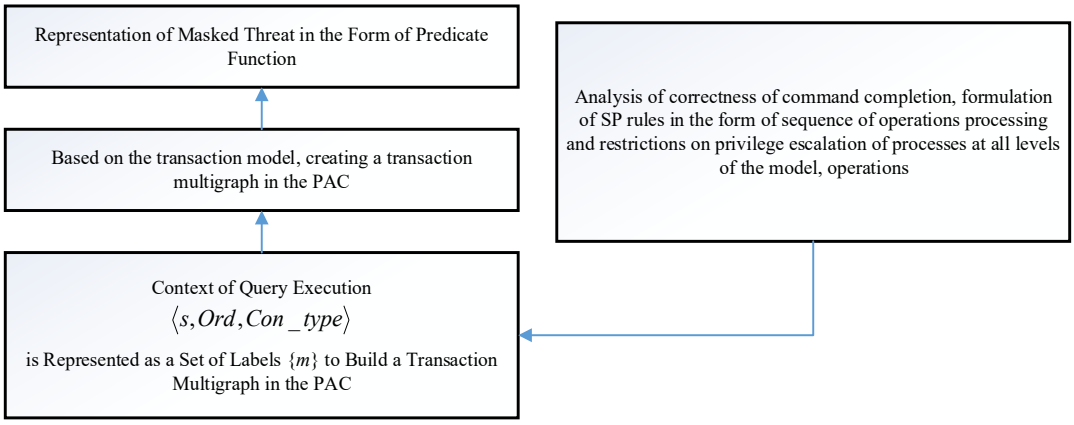

Fig. 3. Block diagram for the predicate process identification method for defense against disguised cyber threats in PAC

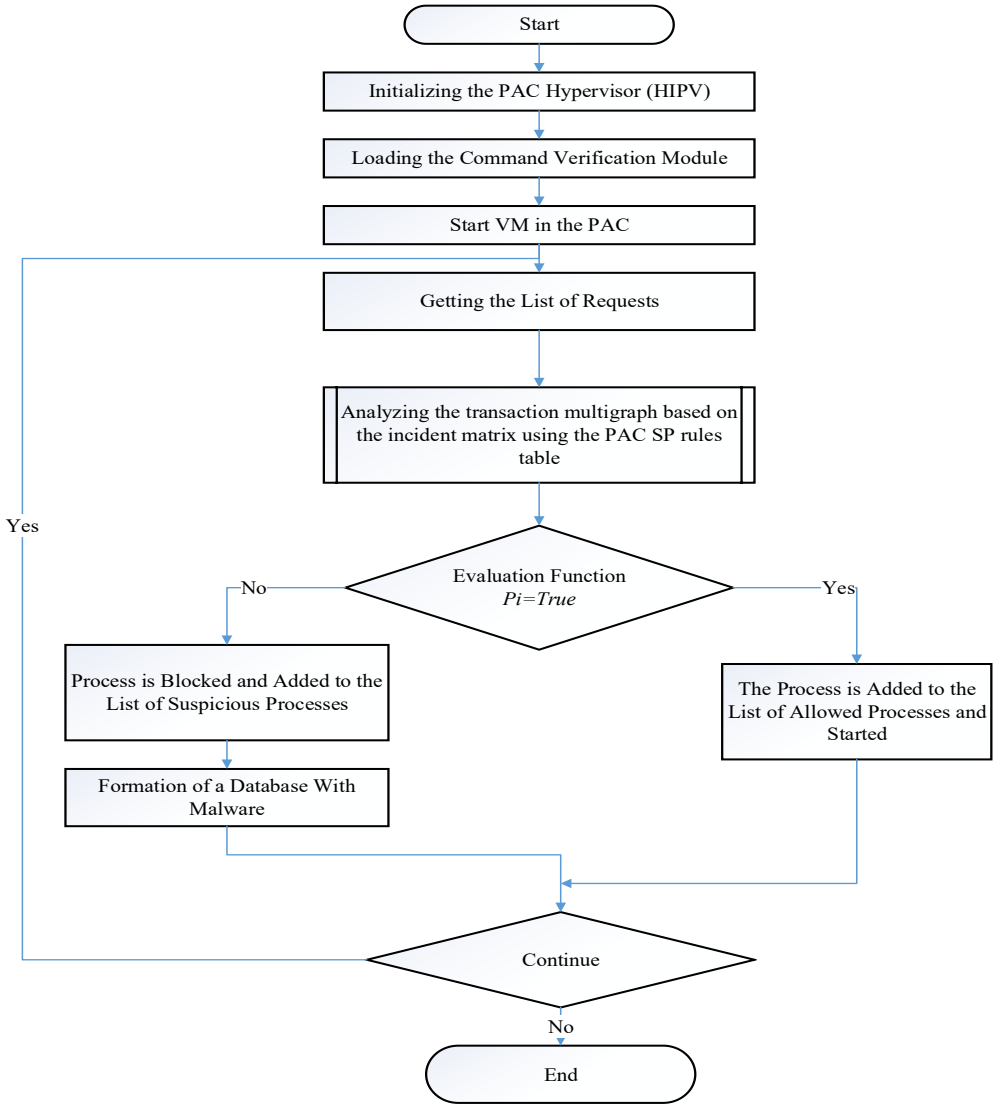

Fig. 4. Block diagram of the algorithm for identifying threats to the university's COLE

The procedure for searching for masked threats corresponds to a cyclic algorithm. In this algorithm, we analyze query lists, based on the value $P_i = true$ - state estimation function.

Table I shows an example fragment of the matrix for the knowledge base (KB) generated as a result of the algorithm presented in Figure 3. The use of fuzzy variables allowed a broader description of the characteristics of potentially dangerous cyber threats to the PAC. Such work, in the end, contributes to the solution of the problem of constructing the decisive rules that determine the state of PAC in the case of detection of cyber threats.

In Tables I and II, the following notations are adopted: EUM^* - set of entities within the set of PAC nodes um^*; Sub - set of PAC subjects; RDN - set of edges of the PAC state graph S_R (SESG), including those corresponding to users' access rights to EUM^*; ADN - PAC SESG, which correspond to the rights of access to EUM^*; MIF - PAC SESG, which correspond to information flows between EUM^* ($um^* \subset EUM^*$); IR - hierarchy function EUM^*.

For each of the relations of the inference tree, fuzzy KBs are constructed, which represent a set of fuzzy "if-then" rules. These rules define the relationship between the incoming and outgoing variables in the evaluation of PAC IS. A rule is activated if the truth of its condition is greater than zero.

The method of composing a decisive rule $\text{gov}(p_{\text{axi}})$ for determining the state of systems S_R in case of a threat to IS, based on the procedure of analyzing the criticality of individual elements of the information system, and PAC in particular, was described in more detail in [19]. Table 1 shows a fragment of the KB formed for recognizing cyber threats to PAC.

This method includes the following main stages:

1) trusted users who have the right of access to the entities of PAC (e.g., to information arrays - $M_{k\,\text{inf}}$) are defined for each node of PAC $um^* \subset EUM^*$;

2) sets EUM^*, Sub and function IR do not change on all the trajectories of the PACU state graph;

3) To gain access to an entity by an infringer Sub_x of an entity's ownership rights Sub_1, he usually needs to gain access

not only to an entity EUM_z^*. A write/read access right to some entity $\text{eum}_l \in \text{EUM}^*$ is also required . This entity acts as an interface or port of some process entity $pro \in Sub$, which performs the granting of access rights SDN_i based on data about EUM^*;

4) entities EUM_z^* and eum_l are associated with a subject pro_r^m; entities eum_l and pro_r^m are usually hosted on a single node of the PAC. Entities EUM_z^* and EUM_y^* may be hosted on different nodes of the PAC;

5) the decisive rule *gov(x)* describing the states of the PAC can be represented in this form, see Table II.

TABLE I
FRAGMENT OF THE KB FORMED FOR DETECTING CYBER THREATS TO PAC

Attributes	Signs of threat (attack) to PAC	Informativeness of the feature value	Universum	Terms for linguistic evaluation of the $\phi_u,\ldots,\phi_v$ states of the IS of PAC
Multiple classes of cyber threats to PACs $KL=\{KL_1,\ldots,KL_n\}$, Multiple targets of an IS intruder $PA=\{PA_1,\ldots,PA_z\}$, A set of numbers of cyber threats that an intruder must implement in order to achieve a pa- ternal goal $B_{p_a}=\{b_{p_{a1}},\ldots,b_{p_{au}}\}$, Multiple IS asset numbers $N_j^{p_a}=\{n_1^{p_{a1}},\ldots,n_j^{p_{au}}\}$ for PAC, Multiple possible perpetrators $U=\{u_1,\ldots,u_g\}$, Multiple recorded IS incidents for the PAC $NIS=\{nis_1,\ldots,nis_f\}$, Set of possible variants of threat realization (attacks) $AT=\{AT_1,\ldots,AT_q\}$, Set of algorithms (AL) of threat recognition for IS PAC $MC=\{MC_1^{AL},\ldots,MC_j^{AL}\}$, and etc	A set of signs of threat (attack) realization within the class KL $\text{p}_{\text{ax}}=$ $=\{\text{p}_{\text{ax}1},\ldots,$ $\text{p}_{\text{ax}_{\text{MI}}}\}.$	Based on NIS and terms $\phi_u,\ldots,\phi_v$ $-1\le \text{IZ}_{\text{p}_{\text{axj}}}\le 1$	$[0,\text{N}_a]$ or [0,1], c. u.	Non-critical, critical or for threats identified, partially identified, not identified, not identified or fixed, not fixed, not fixed, etc.
System Status (PAC) $\text{S}_{\text{IK}}=\{\text{S}_{\text{IK}_1},\ldots,\text{S}_{\text{IK}_m}\}$				
Methods of counteracting threats $\text{D}_{33\text{i}}=\{\text{D}_{33\text{i}_1},\ldots,\text{D}_{33\text{i}_r}\}$				
Rule for the output tree *IF* ($\text{KL}_1\vee\ldots\vee\text{KL}_n\vee S_{IK_J}\vee\ldots\vee S_{IK_m}$) *THEN* D_{33i_r} and $\mu^{d_j}(\text{S}_{\text{IK}_i})=\bigvee_{p=1}^{h_j}\left[\mu^{y_1}(y_1)\wedge\ldots\wedge\mu^{\phi_v}(\phi_v)\right]$, $p=\overline{1,h_j}$, $j=\overline{1,MI}$, where $\mu^{y_1}(y_1),\ldots,\mu^{\phi}(\phi_u)$, $\mu^{\phi}(\phi_v)$ – belonging functions y_1, $\phi_u,\ldots,\phi_v$ to their fuzzy terms; y_1 – IS PAC state {below critical, critical, above critical, high}; $\vee$ – logical «OR», $\wedge$ – logical «AND», as operations *max* and *min*.				

TABLE II
DECISIVE RULE FOR DETERMINING THE STATUS OF A PAC IN THE EVENT OF A CYBER THREAT DETECTION

Rule	The initial state of the system, S_R	The resulting state of the system, S'_R
$gov(p_{axi}) = = (Sub_x, Sub_y, EUM^*_z, eum_l, pro^m_r)$	$Sub_x, Sub_y, pro^m_r \in EUM^*, eum_l,$ $EUM^*_z \in EUM, eum_l \in pro^m_r,$ $(Sub_x, eum_l, write_r / read_r \in RDN),$ $EUM^*_z \in Sub_y \text{ or } Sub_x = Sub_y,$ $or\ (EUM^*_z, Sub_x, write_m / read_m)$ $\in MIF, KL, MC \in AL(KL)$	$S_R = S'_R, EUM^* = EUM'^*,$ $ADN = ADN', IR = IR',$ $MIF = MIF', RDN' = RDN'(Sub_x,$ $Sub_y), KL \in (KL_1,...KL_l),$ $MC \in AL$ $(KL \in (KL_1,...KL_l))$

The algorithm for identifying threats to the PAC (see Fig. 3) and the decisive rule for determining the state of the PAC in the event of a cyber threat has been implemented in the software product (SP) "Threat Analyzer".

This program product was previously described in [19]. Some results of its tests are shown in Table III.

V. EXPERIMENTAL STUDIES

Experimental studies of the method of detection of cyber threats for PAC and the software "Threat Analyzer" were conducted on the basis of private clouds of four major universities - two in Ukraine and two in Kazakhstan.

When conducting experimental considered the possibility of detecting malware - Rootkit:W232/HacDef, Rootkit:Rustock, Rootkit Win32.Ntldrbot:Rustock.C. The effectiveness of the software "Threat Analyzer" to detect these threats was compared with the capabilities of two commercial systems. The quantitative indicators of successful detections and errors of the first and second type were evaluated. The results are shown in Table III.

TABLE III
COMPARISON OF THE RESULTS OF THREAT ANALYZER WITH SIMILAR SOFTWARE

Software name	Rootkit: W232/HacDef	Rootkit: Rustock	Rootkit: Win32.Ntldrbot (Rustock.C)
ESET Internet Security	+	+	+
Norton Internet Security	+	+	+
Software «Threat Analyzer»	+	+	-

Table III is labeled with the appropriate symbols: "+" - successful detection of a cyber threat to the PAC: "-" - detection failure.

VI. DISCUSSION OF THE RESULTS

As indicated in Table 3, traditional methods of PAC control are effective at the initial levels of the VM process interaction model within the HIPV of the private academic cloud. A comparative assessment of the threat identification system for the PAC demonstrated the commendable efficacy of the developed "Threat Analyzer" software. This software is capable of detecting not just threats of the Rustock.C type.

The advantages of discrete threat recognition procedures (DTRP) are: obtaining the classification function of the cyber threat with the minimum level of classification error; the possibility of using linear classifiers to work with nonlinear data; the ability to work with heterogeneous complex structured data; when changing the structure of the considered data (signs of cyber threats) it is sufficient to replace only the decisive rule $gov(p_{axi})$ without replacing the DTRP algorithm itself.

Among the shortcomings of the research is the fact that so far the experiments on threat detection have covered only a relatively small range of threats characteristic of PACs. Work will continue in this direction.

VII. ACKNOWLEDGEMENTS

The research was carried out within the framework of the IRN project AP19678846 "Increasing the efficiency of hybrid and distance forms of educational process organization based on the development of higher education infrastructure in the conditions of digital transformation".

CONCLUSION

It has been determined that within any university's Cloud-Oriented Learning Environment (COLE), there exist interface levels of interaction among various modules (or components) of the cloud infrastructure. These interaction levels can enable the exploitation of undocumented features, especially for attackers aiming to target the university's Private Academic Cloud (PAC).

In this paper, a method for detecting cyber threats to the private academic cloud based on discrete threat detection procedures using the apparatus of logic functions and fuzzy sets was improved. This improved the efficiency of cyber threat detection in PAC. The solutions proposed in this thesis ultimately contribute to a guaranteed countermeasure against the introduction of malware in PAC.

REFERENCES

[1] Kiv, A. E., Shyshkina, M. P., Semerikov, S., Striuk, A. M., Striuk, M. I., & Shalatska, H. M. (2020, July). CTE 2019–When cloud technologies ruled the education. In Ceur workshop proceedings (Vol. 2643, pp. 1-59).

[2] Paxton, N. C. (2016, November). Cloud security: a review of current issues and proposed solutions. In 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC) (pp. 452-455). IEEE. https://doi.org/10.1109/CIC.2016.066

[3] Wang, Y., Deng, S., Lin, W. M., Zhang, T., & Yu, Y. (2010, October). Research of electric power information security protection on cloud security. In 2010 International Conference on Power System Technology (pp. 1-6). IEEE. https://doi.org/10.1109/POWERCON.2010.5666728

[4] Lewis, K. (2017). Virtual private cloud security. In Computer and Information Security Handbook (pp. 937-942). Morgan Kaufmann.

[5] Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2023). Cloud security threats and solutions: A survey. Wireless Personal Communications, 128(1), 387-413. https://doi.org/10.1007/s11277-022-09960-z

[6] Chavan, P., Patil, P., Kulkarni, G., Sutar, R., & Belsare, S. (2013, December). IaaS cloud security. In 2013 International Conference on Machine Intelligence and Research Advancement (pp. 549-553). IEEE.

[7] Vaquero, L. M., Rodero-Merino, L., & Morán, D. (2011). Locking the sky: a survey on IaaS cloud security. Computing, 91, 93-118. https://doi.org/10.1007/s00607-010-0140-x

[8] Velev, D., & Zlateva, P. (2011). Cloud infrastructure security. In Open Research Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2010, Sofia, Bulgaria, March 5-6, 2010, Revised Selected Papers (pp. 140-148). Springer Berlin Heidelberg.

[9] Kankhare, D. D., & Manjrekar, A. A. (2016, December). A cloud based system to sense security vulnerabilities of web application in open-source private cloud IAAS. In 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT) (pp. 252-255). IEEE. https://doi.org/10.1109/ICEECCOT.2016.7955225

[10] Rajesh, M. (2017). A systematic review of cloud security challenges in higher education. The Online Journal of Distance Education and e-Learning, 5(1).

[11] Alimboyong, C. R., & Bucjan, M. E. (2021). Cloud Computing Adoption among State Universities and Colleges in the Philippines: Issues and Challenges. International Journal of Evaluation and Research in Education, 10(4), 1455-1461. https://doi.org/10.11591/ijere.v10i4.21526

[12] Chatterjee, P., Mukherjee, S., Bose, R., & Roy, S. (2021). A Review on Information Security in Cloud Based System during Covid-19 pandemic. Brainwave, Brainware University, 2(1), 60-69.

[13] Najm, Y. A., Alsamaraee, S., & Jalal, A. A. (2022). Cloud computing security for e-learning during COVID-19 pandemic. Indonesian Journal of Electrical Engineering and Computer Science, 27(3), 1610-1618. https://doi.org/10.11591/ijeecs.v27.i3.pp1610-1618

[14] Hui, S. C., Kwok, M. Y., Kong, E. W., & Chiu, D. K. (2023). Information security and technical issues of cloud storage services: a qualitative study on university students in Hong Kong. Library Hi Tech. https://doi.org/10.1108/LHT-11-2022-0533

[15] Mulyar, I. V., Miroshnichenko, O. V., Krasnik, A. V., & Solodeeva, L. V. (2018). Protection against hidden threats in the cloud computing environment. Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University, (59), 115-126.

[16] Molyakov, A. S., Zaborovsky, V. S., & Lukashin, A. A. (2015). Model of hidden IT security threats in the cloud computing environment. Automatic Control and Computer Sciences, 49, 741-744.

[17] Molyakov, A. S. (2014). Means of countering hidden threats to information security in the cloud computing environment (Doctoral dissertation, St. Petersburg State Polytechnic University).

[18] Zaborovsky, V.S. and Lukashin, A.A., High performance protected cloud, Otkrytye Sist., SUBD, 2013, no. 6, pp. 10–13

[19] Lakhno, V., Kazmirchuk, S., Kovalenko, Y., Myrutenko, L., Zhmurko, T. Design of adaptive system of detection of cyber-attacks, based on the model of logical procedures and the coverage matrices of features (2016) Eastern-European Journal of Enterprise Technologies, 3 (9), pp. 30-38. https://doi.org/10.15587/1729-4061.2016.71769

[20] Lakhno, V. *et al.* (2023). The Model of Server Virtualization System Protection in the Educational Institution Local Network. In: Shakya, S., Papakostas, G., Kamel, K.A. (eds) Mobile Computing and Sustainable Informatics. Lecture Notes on Data Engineering and Communications Technologies, vol 166. Springer, Singapore. https://doi.org/10.1007/978-981-99-0835-6_33

[21] Lakhno, V., Akhmetov, B., Mohylnyi, H., Blozva, A., Chubaievskyi, V., Kryvoruchko, O., & Desiatko, A. (2022). Multi-criterial optimization composition of cyber security circuits based on genetic algorithm. Journal of Theoretical and Applied Information Technology, 100(7), 1996-2006. ISSN 1992864

[22] B.S. Akhmetov, V. Lakhno, B.B. Akhmetov, A. Zhilkishbayev, N. Izbasova, O. Kryvoruchko, A. Desiatko, Application of a Genetic Algorithm for the Selection of the Optimal Composition of Protection Tools of the Information and Educational System of the University, Procedia Computer Science, Volume 215, 2022, Pages 598-607, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2022.12.062.

[23] Valerii Lakhno, Zhuldyz Alimseitova, Yerbolat Kalaman, Olena Kryvoruchko, Alona Desiatko, and Serhii Kaminskyi. Development of an Information Security System Based on Modeling Distributed Computer Network Vulnerability Indicators of an Informatization Object. International Journal of Electronics and Telecommunications, 2023, VOL. 69, NO. 3, PP. 475-483 https://doi.org/10.24425/ijet.2023.146495

[24] Lakhno, V. *et al.* (2021). Information Security Audit Method Based on the Use of a Neuro-Fuzzy System. In: Silhavy, R., Silhavy, P., Prokopova, Z. (eds) Software Engineering Application in Informatics. CoMeSySo 2021. Lecture Notes in Networks and Systems, vol 232. Springer, Cham. https://doi.org/10.1007/978-3-030-90318-3_17