Studies on Cloud-based Cyber Incidents Detection and Identification in Critical Infrastructure

Sergiy Gnatyuk[a,b], Rat Berdibayev[c], Zhadyra Avkurova[d], Oleksii Verkhovets[b], and Madina Bauyrzhan[e]

[a] *National Aviation University, 1 Liubomyr Huzar ave., Kyiv, 03058, Ukraine*
[b] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 Maksym Zaliznyak str., Kyiv, 03142, Ukraine*
[c] *Almaty University of Power Engineering and Telecommunication, 126/1 Baytursynuli str., Almaty, 050013, Kazakhstan*
[d] *L. N. Gumilyov Eurasian National University, 2 Satbayev str., Nur-Sultan, 010000, Kazakhstan*
[e] *Satbayev University, 22a Satbayev str., Almaty, 050000, Kazakhstan*

Abstract

Cloud and other advanced technologies are implementing in various ICT infrastructures. It has led to increased attention to the problems of cyber threats, the growth of which is inseparably linked with the growth of ICT. In this paper, the analysis of the existing models, systems, and methods for cyber threats detection in critical infrastructure was carried out for their disadvantages defining. A model of cloud service has been developed; it allows to ensure the security of cloud service and conduct appropriate simulations. An improved method for cyber incidents detection has been developed, it allows to detect of cyber threats in cloud services and classify them. The developed method was experimentally investigated using the NSL-KDD dataset. It was proved the correctness of its work and the possibility of application in cloud services as well as increase efficiency of cloud system security. A cloud service model has been developed that can be used to build cloud services based on various architectures. In the future, based on the proposed method and model, appropriate tools for detecting and classifying cyber threats in cloud services can be developed. It can be an autonomous functional unit of SIEM as well as other instrumental tools of CSIRT/SOC in critical infrastructure.

Keywords

Cloud service, cybersecurity, cyber incident, critical infrastructure, detection, identification, architecture, NSL-KDD dataset.

1. Introduction

Today different world states define energy, transport, communications, gas, and oil industry, and other sectors as important units of critical infrastructure (Fig. 1). The traditional technologies and processes are becoming progressively more connected to modern digital technologies and ICT networks. This increasing digitalization makes the various system smarter and enables consumers to better benefit from innovative services. Digitalization creates significant risks as increased exposure to cyberattacks and cyber incidents potentially jeopardize the security and the privacy of consumer data [1]. The protection of critical infrastructure is essential for states because the well-being of their societies depends on their good functioning. An attack on it or a disruption can cause serious problems to the citizens and can jeopardize the national security of the state. For this reason, today critical infrastructure protection is a key issue [2].

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: s.gnatyuk@nau.edu.ua (A.1); r.berdybaev@aues.kz (C.2); zhadyra.avkurova.83@mail.ru (D.3); o.verkhovets@gmail.com (B.4); madina890218@gmail.com (E.5)
ORCID: 0000-0003-4992-0564 (A.1); 0000-0002-8341-9645 (C.2); 0000-0002-0706-6075 (D.3); 0000-0003-5233-9774 (B.4); 0000-0002-8287-4283 (E.5)

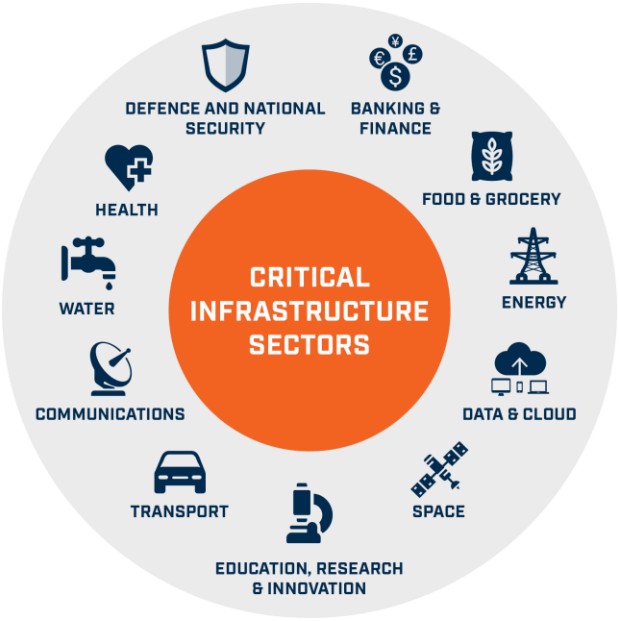

Figure 1: Sectors of critical infrastructure by Huntsman

In various critical infrastructures cloud services using can deploy users' 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 cybersecurity 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 (incident) detection (MCD), IDS/IPS systems, cyber incident response modules, and others [3].

Cyber threat is any circumstance or event that may cause a breach of cybersecurity policy and/or damage to an automated system [4–6]. The main purpose of cybersecurity is to prevent the implementation of existing cyber threats, which are the sources of the following risks [7–10]:

1. Loss of intellectual property.
2. Violation of compliance and regulations.
3. Compromising credentials and authentication.
4. API threats.
5. Hacking accounts.
6. Improper usage of cloud services.

2. Review of Related Papers and Problem Statement

2.1. Cloud Security

Cloud computing systems have a multi-level architecture of different services and levels of management. Security issues for the SaaS platform can generally be divided into two categories: attacks on development tools and attacks on management tools. In general, all threats can be divided into three groups:

1. Threats to data confidentiality.
2. Attacks on the interface.
3. SSH attacks.

Security issues for the IaaS and PaaS platforms are grouped into four classes: attacks on cloud services, attacks on virtualization, attacks on unified computing, and attacks on SLAs [11, 12]. Table 1 shows a multi-level classification of threats for the three layers of clouds, which are the first level. At the next level are cloud services, and at the third – the types of attacks on these services [13].

Table 1. Multilevel classification of data security threats (incidents) in cloud computing

Layer of cloud (service)	Cloud service	Security threat	Attack type	Risk value
SaaS	Web service	Data security	Confidentiality	Medium
		Interface attack	Signatures attack	Low
			Attacks on users credentials	Medium
	API	SSH attacks	Attacks on API keys	Medium
			Attacks on users credentials	Medium
IaaS and PaaS	Virtualization platform	Hardware-level virtualization	ARP spoofing on virtual switching	High
			MAC spoofing on virtual switching	High
		Software level virtualization	Hacking on computing	Low
Development services	Cloud software	Harmful software	Scripts	High
	Computing services	Unified computing attacks	Attacks during data processing	Low
		SLA attacks	Hacking	High

2.2. Related Papers on MCD

There are many MCDs, but they all use very similar techniques for direct detection. A significant disadvantage of most of them is that they are described only theoretically and have no practical confirmation (verification).

1. Method for cyber threat recognition based on fuzzy feature clustering [14, 15]. The essence of splitting objects that contain signs of anomalies (cyberattacks) into a class of sets of the same type in terms of cybersecurity lies in splitting sets of objects into subsets. The method involves the usage of machine learning. Traditional fuzzy clustering algorithms use a given number of partition clusters as input parameters, and some of them also use a given cluster fuzzy index in the space of signs of vulnerabilities, anomalies, NSD threats, and cyberattacks [16, 17]. Based on the information criterion of functional efficiency for the IP, a mechanism for adjusting the parameters of the algorithm for clustering threat signs can be implemented.

2. Method for detecting cyber threats using Big Data technology [18]. Data management and expertise methods such as biometric authentication protect against cyberattacks by providing security solutions to the massive protection of data volumes. By analyzing Big Data logs, we can prevent cyber threats by monitoring data. When Big Data analysis is combined with JIT (Just in Time) analysis, it collects information on machines that have an open connection to locations outside the LAN. It also predicts future attacks and provides information about previous attacks that may have taken place on your system. IBM has developed a big data solution that protects data from threats and fraud. IBM's solution detects risk and intrusion when analyzing structured and unstructured data. QRadar correlates in real-time, detects anomalies and reports for immediate threat detection, and sends rich security data to IBM Big Data products such as IBM InfoSphere BigInsights. Large datasets need to be reduced to successfully detect anomalies.

3. Method for detecting cyber threats using the analysis of social networks [19]. Among the main classes of methods used in ACC, we can distinguish the following: methods of graph analysis,

statistical methods, data mining, methods of optimization theory, and algorithm theory. It is also convenient to single out the methods of semantic analysis and text analysis. In this case, it is necessary to verify whether the system supports the language in which users of the analyzed social network communications. These methods are used to identify the following major threats: network spam; threats to social engineering; password theft and phishing; web attacks; leakage of information and compromising the behavior of company employees; Advanced Persistent Threat (APT) attacks.

4. Method for cognitive security using artificial intelligence [20]. It is the concept of a self-defense network that identifies a potential threat on the Internet and takes appropriate action to prevent "confidential data from being compromised". At the same time, you use a combination of a number of modern technologies to identify and analyze key threats (both external and internal to the client) using special techniques for analyzing real-time data behavior.

5. Method for detecting cyber threats using a structured behavioral model [21]. The method is based on the analogy of comparing natural language and network traffic. First, the Trace Sequence of the captured network traffic is determined with the parameters: active text, active grammar, active vocabulary, and ratio. The next step is to start processing the captured sequence using DBSCAN—a spatial data clustering algorithm where noise is present. Next, the data from the analysis of the captured piece of traffic is compared with the normal behavior of traffic that was obtained in an isolated environment and is called the reference. Having certain differences results in the detection of cyber threats.

6. Method for "deep analytics" [22, 23]. This method is a combination of popular and effective methods (predictive analytics, descriptive analytics, graph analysis, analysis of unstructured information, optimization), which together give the desired result—the detection of cyber threats or anomalies. Examples of method implementation: detection of anomalies; statistical threat profiles; relationship analysis.

7. Method for detecting cyber threats of Yu. Malachi [24]. The system and method of detecting a cyber threat in accordance with implementations of the present invention include automatic detection of resources in the network, resource detection unit, emulation, fake asset creation unit, at least one resource detected in the network, associating a trap sensor with malware with emulation resource and detection by malicious trap sensor, malware related to the emulated resource. The system and method may also include downloading data related to the detected malware on the server, analyzing the downloaded data on the server to obtain the analysis result, and performing one or more actions based on the analysis result.

8. Radar Services method for detecting and counteracting cyber threats [25]. The method is based on the use of many systems for analysis of signature and behavioral analysis of network traffic and next-generation isolated software technologies for analysis of all incoming e-mails; advanced correlation engine that analyzes the network traffic and events that use statistical models, recursive methods, and machine learning to differentiate normal and abnormal behavior and identify patterns; the usage of a risk and safety management team that analyzes verifies and aggregates all findings.

9. Network streaming and threat detection approach [26]. Numerous studies have been conducted on real-time threat detection systems. The problem of processing large amounts of data on the network traffic of corporate systems, while providing real-time monitoring and detection, was considered, which remains unresolved. In particular, they introduced and evaluated a flow-based threat detection system that can quickly analyze overly intensive real-time network traffic data using streaming flow-based clustering algorithms to detect abnormal network actions.

10. SANS company cyber threat detection, prevention, and control system [27]. This system is described only theoretically (in the form of recommendations), and contains 5 aspects: use of security measures based on end-to-end visibility; avoid excess information; use security solutions that perform real-time analysis; reduce latency within the network; introduction of "deep" protection.

11. Method for data collection, processing, analysis, and storage for monitoring cyber threats and their notification to users [28]. The system collects intelligence data from multiple sources and then pre-processes the intelligence data for further analysis by the intelligence analyst. The analyst reviews the intelligence and determines if it is appropriate for the client to sign a cyber threat alert service. The system reforms and collects intelligence data and automatically transmits intelligence data through many delivery methods.

12. Method for planning the structure of cyber threats and their application to reduce the impact of cyber threats [29]. A security system consisting of a computer, memory, data storage, containing a dictionary of the intellectual capacity of cyber-threats and a technological dictionary; and an application stored in memory. When executed by a computer, the program generates a report that identifies the intent of the cyber threat and identifies the cyber threat technology, in which the intent of the cyber threat is selected from several intentions for the cyber threat listed in the dictionary of cyber threat imposition and in which cyber threat technology is selected from the technology dictionary.

After the analysis of known MCDs [14–29], it is clear that not all of these methods have been qualitatively and experimentally studied. Almost half of them have high requirements for computing resources and are not easy to implement, and therefore are described only theoretically. In addition, due to the technology of the method itself, not all algorithms have the ability to log new, not yet assigned to any category of cyber threats. Also, only fuzzy feature-based clustering, Cognitive Security Method, Network Streaming and Threat Detection System, MCD of SANS company, and MCD using cyber threat planning have real-time cyber threat detection. In the review of the literature for each method was not said that the study was also conducted in cloud computing systems, but indicated the possibility of such implementation for the methods: MCD based on fuzzy clustering of features, MCD using Big Data technology, the method of "deep analytics" and Network streaming and threat detection system. In general, this analysis indicates the problem of detecting cyber threats in cloud environments of any type and services of any type.

2.3. Problem Statement

The main purpose of this work is to develop a method for detecting cyber threats in cloud services. To achieve this purpose we need to solve the following tasks:

1. Develop a model of cloud service and based on it the MCD to ensure the security of cloud services by further neutralizing the identified threats;
2. Experimentally investigate the MCD to verify its correct operation and the possibility of application in cloud services.

3. Theoretical Background of Method Development

3.1. Technological Architecture of Secure Cloud Service based on Cloud Computing Technology

Cloud environment in which the MCD will be introduced in this section. The technology architecture is based on the recommendations of Cisco, which has developed its progression of the evolution of cloud data centers:

1. Consolidation and aggregation of data center assets.
2. Abstraction, is a key phrase because the assets of the data center are abstracted from the services that are 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.

In general, the completed architecture contains not only components of the structure, but also is regulated by different types of service and regulatory requirements.

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).

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 [25]. The key to

gaining an advantage from the cloud is to establish a trusted 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.

3.2. Groups of Cyber Threats, Cyber Incidents, and Cyberattacks in the Clouds

One of the most complete descriptions of all cyber threats and attacks that can be implemented is in the KDD database [30]. NSL-KDD is a data set proposed to solve some of the integral problems of the KDD'99 data set mentioned. Although this new version of the KDD dataset is still not without some problems and is not the best guide to existing real networks, and due to the lack of available datasets for network identification systems, it is used as an effective reference dataset, which will help researchers compare different MCD. In addition, the number of entries in NSL-KDD sets and test sets is processed. This advantage makes it available to run experiments without having to accidentally pick a small portion. Thus, the results of the evaluation of different research papers will be consistent and comparable. The NSL-KDD dataset has the following advantages over the initial KDD dataset:

1. It does not include redundant entries in the data set, so classifiers will not be biased for a recurring entry.
2. There are no duplicate records in the proposed test sets; therefore, productivity is not biased by methods that have better detection rates.
3. The number of selected records from each complex group is inversely proportional to the percentage of records in the original KDD dataset. As a result, the classification indicators of different teaching methods change in a wider range, which makes it more effective to accurately assess different teaching methods.
4. The number of entries in the set and test sets is clear, making it possible to experiment on a complete set without having to randomly select a small part.

3.3. Block Diagram of the Proposed Method for Detecting Cyber Incidents

Fig. 2 shows a block diagram of detecting cyber threats in a cloud environment. When the host is connected to the cloud environment, network traffic begins to be generated. Next is the data processing unit (data process), where the network traffic arrives at the behavior analyzer (behavior analyzer), which contains the records of the NSL-KDD database. The analyzer compares the data captured from the network traffic with the database and begins to use classifiers to determine.

The next block to which the data is transmitted is the block of identification and analysis, where the pre-classified threat is analyzed in detail on certain grounds, and it is determined to which elements the threat was directed.

After that, the system issues a warning message that part of the traffic is abnormal, and at the same time begins to check the identified threat with previously found or recorded immediately in the database. If such a match is found, a notification with further actions can be issued (in case of their previous successful application). The last two modules are a record of detailed data about the threat (date, group, whether it was previously identified, etc.) and the formation of a mini-report for review, which shows the overall result.

Taking into account the characteristics of cloud computing systems and ideal cyber threat detection systems, the developed method meets the following requirements:

1. Processing of large-scale dynamic multilevel autonomous computing systems and data processing environments. Clouds are large-scale systems based on virtual machines that are automatically created, transferred, and removed at the user's request at runtime. It is generally assumed that the middleware provider initially reported changes in resources, but in cloud computing involving large networks and systems, it is important to automatically support these changes without

human intervention. To overcome the complexity of its dynamic nature, the process of detecting cyber threats must be able to cope with it without human intervention, which facilitates the monitoring and control of network elements in real-time.

2. Identify various attacks with the least false positives. Due to the growing number of attacks, their complexity, and unpredictability, the system must recognize new attacks and their vulnerable intentions to choose the best response according to the degree of risk and proper prevention. The method should be educational and improve its detection ability over time. It should also be designed to maintain the desired level of performance and security with the least computational resources, as the efficiency of cloud services is based on its computing capabilities.

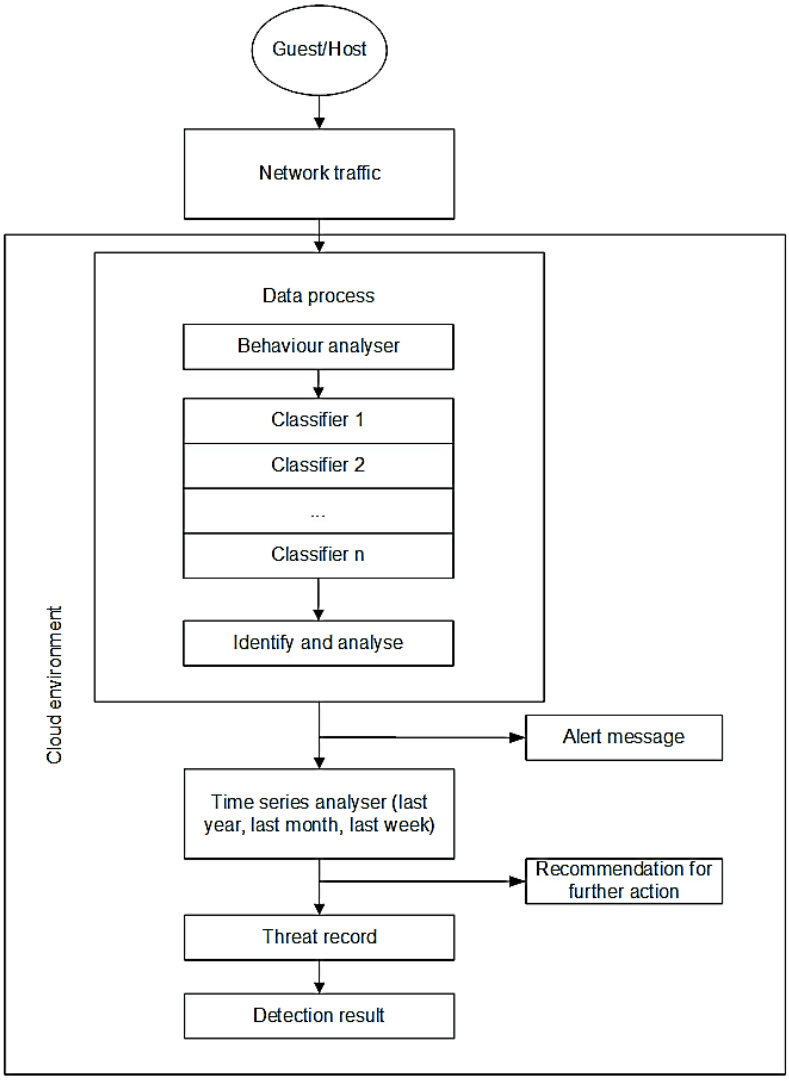

Figure 2: Block diagram of the MCD in the cloud environment

3. Quick detection and warning. Rapid detection and warning is a very important factor in the development of detection methods, as it affects the overall performance of the system and is crucial for the delivery of pre-agreed QoS. A cloud system with multiple administrators should minimize or have no human intervention to avoid wasting time on the administrator's response. It must work in real-time and provide automatic responses to suspicious actions.

4. Autonomous self-adaptation. The cyber threat detection system must be self-configured and adapted to configuration changes, as computing nodes are dynamically added and removed. The development of an appropriate architecture will allow you to determine how alerts should be processed and distributed from the individual detection components while maintaining the topological model of cloud computing. It also facilitates the monitoring and control of network components.

5. Scalability. The MCD must be scalable to efficiently handle the huge number of network nodes available in the cloud and their communication and computational load.

6. Deterministic calculations in the cloud. They provide critical and critical functional services that have specific performance requirements in terms of retention, reliability, and resilience. MCD should not only provide real-time performance but also ensure the negative impact of the deterministic nature of the network.

7. Synchronization of autonomous MCD. Information and actions must be synchronized to detect widespread and simultaneous attacks, to apply appropriate responses, or to change a particular component system or configuration of the entire network and to adopt an appropriate prevention strategy.

8. Resistance to compromise. The MCD must protect itself from unauthorized access or attacks. The IMC must be able to authenticate network devices, authenticate the administrator and verify its actions, protect its data, and block any vulnerabilities that may cause additional vulnerabilities.

4. Experimental Study and Discussion

4.1. Experimental Study using RStudio

Input /output of the experiment: the input data is 20% of the NSL-KDD dataset, the output data are classified data (normal or abnormal—threat).

Experimental environment: open-source development environment for R (programming statistics and RStudio data visualization).

RStudio includes a console, a syntax-highlighting editor that supports direct code execution, and tools for scheduling, logging, debugging, and desktop management.

Fig. 3 shows the working environment of the RStudio tool.

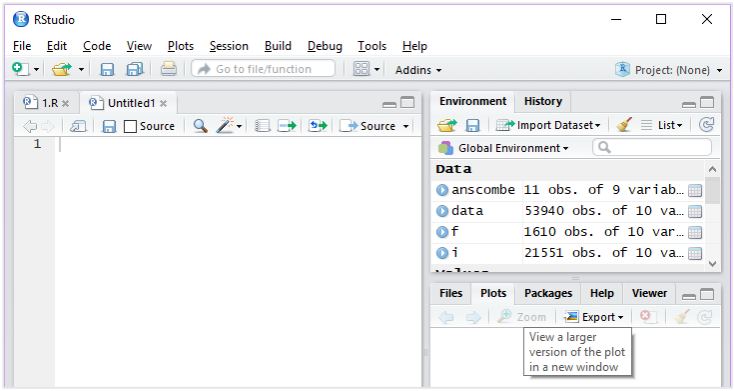

Figure 3: The main working window of RStudio tool

The window is divided into four parts:

1. Working part—for direct writing and running code, there is also a standard toolbar for all tools.

2. After viewing the data—there are tabs of the environment (you can view the loaded data sets and libraries) and history (see versions of the project).

3. Console—to display the results of the written program, and data related to the environment (loading of the library).

4. Field of view of visualized results (diagrams, histograms, etc.).

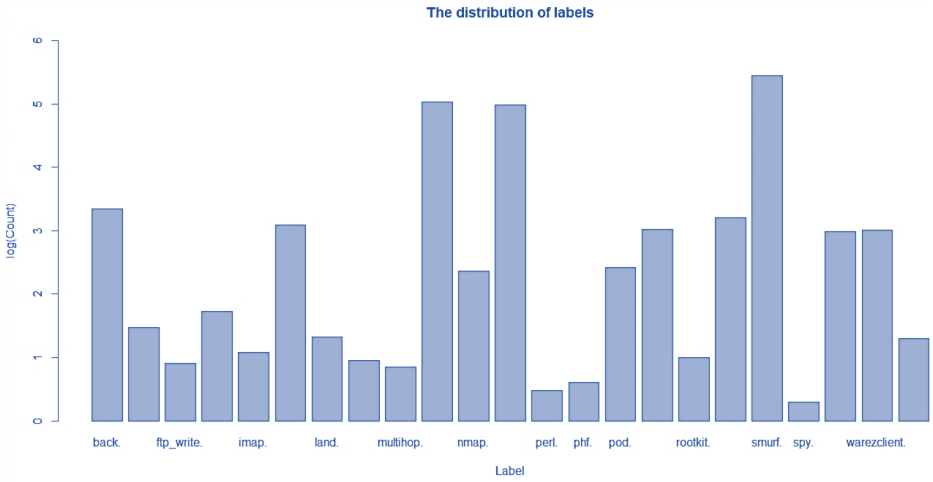

Figure 4: Distribution of types of threats

Stages of research study

Stage 1: Connection of all necessary libraries, loading of a training data set of NSL-KDD database.

Stage 2: Analysis of the test data set. Only 20% of the training data of the NSL-KDD database have 25,191 elements that have 43 features. In Fig. 4 the distribution of types of threats and attacks is shown. As can be seen from Fig. 4 the largest number of attacks is related to the DoS [25].

Stage 3: Direct testing of the method. Next, we test our method using built-in functions and data set. Initially, residual data and duplicates were separated, and separate small data sets were identified. After that, the traffic is analyzed and the normal and anomalous data are determined, as well as the accuracy of the result (Fig. 5).

Stage 4: The result of the experiment. During the experiment, the following results were obtained: the total percentage of threats detected—96.356%, correctly classified—95.89%, incorrectly classified—4.11%.

```
Console G:/OneDrive/STUDY/master work/NSL_KDD-master/NSL_KDD-master/
> print (Detected_cyberthreats)
[1] 96.356
> print (Correctly_Classified)
[1] 95.89
> print (Incorrectly_Classified)
[1] 4.11
> print (NB_accuracy)
[1] 91.6
```

Figure 5: Test results of the MCD

The next subsection contains a study using CloudSim tool and NSL-KDD data set.

4.2. Experimental Study in the CloudSim Simulation System

Input/output of the experiment: the input data is a set of NSL-KDD data and captured network traffic, the output—classified data (normal or abnormal—threat), and the value of the efficiency of the MCD.

Experimental environment: CloudSim simulation system.

CloudSim platform is a generalized and scalable simulation tool that allows full-fledged modeling and simulation of cloud computing systems and infrastructure, including the construction of data centers using the “cloud”. It is an extension of the basic functionality of the GridSim platform, providing the ability to model data storage, web services, resource allocation between virtual machines [31]. Let’s look at the log of the revealed threats which was written down during carrying out modulation (Fig. 6).

```
0,tcp,smtp,SF,1022,387,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,3,0,0,0,0,1,0,1,
255,28,0.11,0.72,0,0,0,0,0.72,0.04,normal,21
0,tcp,telnet,SF,129,174,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0
,255,255,1,0,0,0,0.01,0.01,0.02,0.02,guess_passwd,15
0,tcp,http,SF,327,467,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,33,47,0,0,0,0,1,0,0
.04,151,255,1,0,0.01,0.03,0,0,0,0,normal,21
0,tcp,ftp,SF,26,157,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,1,0,0,0,0,1,0,0,52,
26,0.5,0.08,0.02,0,0,0,0,0,guess_passwd,7
0,tcp,telnet,SF,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,1,0,0,255
,128,0.5,0.01,0,0,0,0,0.66,0.32,mscan,9
0,tcp,smtp,SF,616,330,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,2,0,0,0,0,1,0,1,2
55,129,0.51,0.03,0,0,0,0,0.33,0,normal,18
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,111,2,0,0,1,1,0.02,
0.07,0,255,2,0.01,0.07,0,0,0,0,1,1,neptune,21
0,tcp,telnet,S0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,120,120,1,1,0,0,1,0,0
,235,171,0.73,0.07,0,0,0.69,0.95,0.02,0,neptune,18
37,tcp,telnet,SF,773,364200,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,1
,0,0,38,73,0.16,0.05,0.03,0.04,0,0.77,0,0.07,normal,14
0,tcp,http,SF,350,3610,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,8,8,0,0,0,0,1,0,0,
71,255,1,0,0.01,0.04,0,0,0,0,normal,21
0,tcp,http,SF,213,659,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,24,24,0,0,0,0,1,0,0
,255,255,1,0,0,0,0,0,0,0,normal,21
0,tcp,http,SF,246,2090,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,16,16,0,0,0,0,1,0,
0,35,255,1,0,0.03,0.05,0,0,0,0,normal,21
0,udp,private,SF,45,44,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,505,505,0,0,0,0,1,
0,0,255,255,1,0,1,0,0,0,0,0,normal,15
0,tcp,private,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,204,18,0,0,1,1,0.09
,0.07,0,255,18,0.07,0.07,0,0,0,0,1,1,neptune,21
0,tcp,ldap,REJ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,118,19,0,0,1,1,0.16,0.
```

Figure 6: Log of detected cyber threats

The logs study in RStudio was done to visualize the results: distribution of identified threats and attacks (Fig. 6); diagram of the dependence of the percentage of detection on the type of threat (Fig. 7).

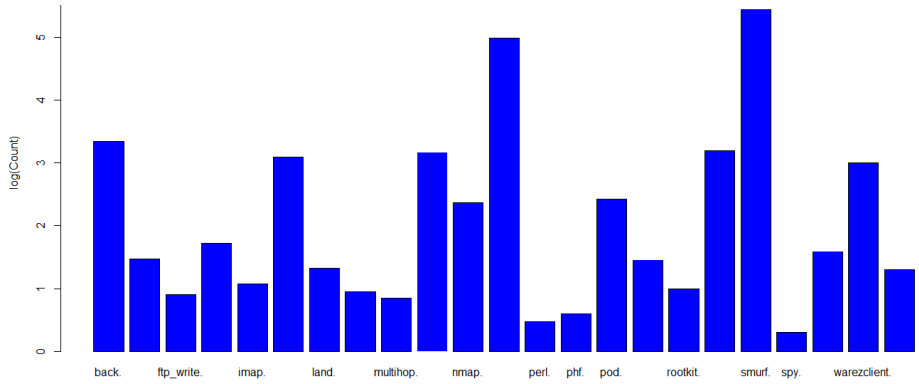

Figure 7: Distribution of identified threats and attacks

As can be seen from Fig. 8 most detected attacks are related to DoS [25].
A comparison of the results of simulations on the CloudSim platform is shown in Table 2.

Table 2. Comparison of simulation results for SIEM detection module

Experiment	MCD connection	Detected threats
1	-	45.87%
2	+	93.89%

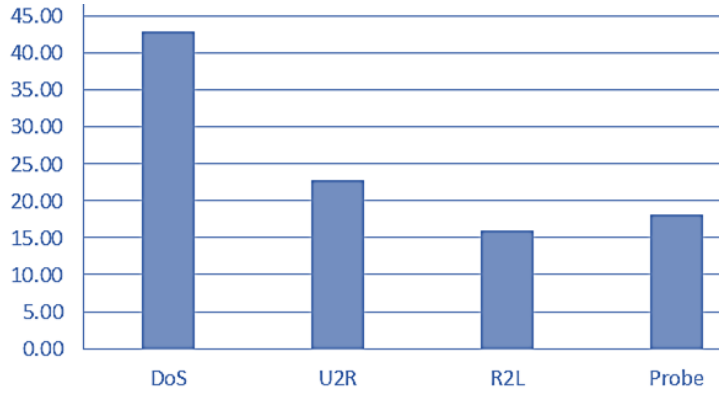

Figure 8: Percentage distribution of identified threats depending on their type

The displayed results indicate that when simulating the data center model without MCD, but provided that there is a built-in threat level security network detector, the level of detected threats is at 45.87%, which indicates insufficient security of the cloud service because it means that if only the built-in anti-attack module is present, less than half of the attacks will be detected. And when conducting simulations with the built-in MCD, the level of detected cyber threats is at the level of 93.89%, which indicates the effectiveness of its work [32–34].

5. Conclusions and Future Research Study

In this paper was defined that the protection and cybersecurity ensuring of critical infrastructure is essential for states because the well-being of their societies depends on its good functioning. The analysis of the existing models, systems, and MCD was carried out, which allowed us 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 MCDs do not implement real-time cyber threat (incident) detection, etc.

A model of cloud service has been developed, which uses technological architecture, high-speed communication, unified structures, and calculations. It allows to ensure the security of cloud services based on cloud computing and conduct appropriate simulations of cloud service functioning.

Improved MCD has been developed, which due to dynamic resources, autonomous self-adaptation, and scalability, and deterministic calculations allows to detect of cyber threats in cloud services and classify them (for example, using the NSL-KDD classifier or other datasets of cyber threats and classifiers).

The developed MCD for cloud services was experimentally investigated using the NSL-KDD database. It has proved the correctness of its work and the possibility of application in cloud services as well as increase efficiency of cloud system security by 48.02 % (the efficiency of detecting cyber threats in cloud service is 93.89%, and without the application of the proposed MCD is 45.87%).

In addition, a cloud service model has been developed that can be used to build cloud services based on the various cloud computing architecture, that can be used in various sectors of critical infrastructure.

In the future, based on the proposed MCD and model, appropriate tools for detecting and classifying cyber threats in cloud services can be developed [35, 36]. It can be an autonomous functional unit of effective SIEM or other instrumental tools of CSIRT / SOC for cybersecurity events correlation and cyber incidents response.

6. Acknowledgment

This research study was conducted with the support of research grant #AP06851243 “Methods, models, and tools for security events and incidents management for detecting and preventing

cyberattacks on critical infrastructures of digital economics" (2020–2022), funded by the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

7. References

[1] Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security, NATO Energy Security Centre of Excellence, Vilnius, 2018.
[2] Cybersecurity in the energy sector, European Commission, Energy Security. URL: https://ec.europa.eu/energy/topics/energy-security/critical-infrastructure-and-cybersecurity_en?redir=1
[3] M. De Jong, L. Hughes, Critical Energy Infrastructure: Identification and Protection. Energy Security: Operational Highlights 11 (2017).
[4] 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 10 (2015) 44–51.
[5] Active security for advanced threats counteraction. URL: http://www.itsec.ru/articles2/target/aktivnaya-zaschita-kak-metod-protivodeystviya-prodvinutym-kiberugrozam
[6] The 6 Major Cyber Security Risks to Cloud Computing. URL: http://www.adotas.com/2017/08/the-6-major-cyber-security-risks-to-cloud-computing/
[7] Google Security Whitepaper for Google Cloud Platform. URL: https://habrahabr.ru/post/183168/
[8] P. Dokas, L. Ertoz, V. Kumar, Data Mining for Network Intrusion Detection, Recent Advances in Intrusion Detection 15 (2014) 21–30.
[9] P. Ahmed, An intrusion detection and prevention system in cloud computing: A systematic review, Journal of Network and Computer Applications 11 (2016) 1–18.
[10] J. P. Anderson, Computer Security Threat Monitoring and Surveillance, Technical Report Contract 36 (1982) 179–185.
[11] G. Carl, G. Kesidis, R. R. Brooks, Suresh Rai, Denial-of-service attack-detection techniques, IEEE Internet Computing 10 (2006) 82–89. doi: 10.1109/MIC.2006.5.
[12] How to build physical security into a data center. URL: http://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html?page=3
[13] V. Chatzigiannakis, G. Androulidakis, M. Grammatikou, B. Maglaris, A Distributed Intrusion Detection Prototype Using Security Agents, in: Workshop of the HP OpenView University Association, 2004, pp. 14–25.
[14] T. Abraham, IDDM: intrusion detection using data mining techniques, DSTO Electronics and Surveillance Research Laboratory, Salisbury, S. Aust 9 (2001) 30-39.
[15] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Yu. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, 2018. CEUR-WS.org, online CEUR-WS.ORG/Vol-2255/paper18.pdf
[16] M. Chouhan, H. Hasbullah, Adaptive detection technique for Cache-based Side Channel Attack using Bloom Filter for secure cloud, in: 3rd International Conference on Computer and Information Sciences (ICCOINS), 2016, pp. 293–297.
[17] Z. Hu, S. Gnatyuk, O. Koval, V. Gnatyuk, S. Bondarovets, Anomaly Detection System in Secure Cloud Computing Environment, International Journal of Computer Network and Information Security (IJCNIS) 9 (2017) 10–21.
[18] H.-H. Li, C.-L. Wu, Study of Network Access Control System Featuring Collaboratively Interacting Network Security Components, International review on computers and software 8 (2013) 527–532.
[19] S. Dilek, H. Çakır, M. Aydın, Applications of artificial intelligence techniques to combating cyber crimes: A review, International Journal of Artificial Intelligence & Applications 6 (2015) 21–39.

[20] How Big Data Can Improve Cyber Security, Online access mode, URL: https://csce.ucmss.com/cr/books/2017/LFS/CSREA2017/ABD3239.pdf
[21] L. Kirichenko, Cyber threats detection using social networks analysis, International Journal of Information Technologies & Knowledge 11 (2017) 23–32.
[22] Cisco creates self-defending networks for cyber threats detection. URL: https://nag.ru/news/newsline/30762/v-cisco-sozdayut-samooboronyayuschuyusya-set-dlya-vyiyavleniya-kiberugroz.html
[23] Y. Xiaohua, Early Detection of Cyber Security Threats using Structured Behavior Modeling, ACM Transactions on Information and System Security 5 (2013) 10–35.
[24] Methods for deep analytics to counteract of modern threats. URL: http://bis-expert.ru/sites/default/files/archives/2016/bis9_konovalov.pdf
[25] S. Bondarovets, O. Koval, S. Gnatyuk, System for anomalies detection for cellular networks provider based on Big Data concept, Information Technology and Security 4 (2016) 44–53.
[26] Y. Malachi, System and method for cyber threats detection, № WO2015159287, release date 22.10.2015.
[27] Z. Hassan, R. Odarchenko, S. Gnatyuk, A. Zaman, M. Shah, Detection of Distributed Denial of Service Attacks Using Snort Rules in Cloud Computing & Remote Control Systems, in: 5th International Conference on Methods and Systems of Navigation and Motion Control, October 16-18, 2018. Kyiv, Ukraine, 2018, pp. 283–288.
[28] A. Byrski, M. Carvalho, in: Computational Science – ICCS, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 584–593.
[29] Z. Zhang, Hide: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification, IEEE Workshop on Information Assurance and Security 16 (2001) 85–90.
[30] C. Edwards, S. Migues, R. Nebel, D. Owen, System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers, US20020038430A1, 2002.
[31] J. P. Watters, F. Doyle, H. Peltokangas, M. Keane, System and method of cyber threat structure mapping and application to cyber threat mitigation, 2017. Patent No. US9749343B2, Filed 03.04.2014, Issued 29.08.2017. https://patents.google.com/patent/US9749343B2/en?oq=US9749343B2.
[32] K. Vipin, K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset, International Journal of Soft Computing and Engineering 3 (2013) 332–340.
[33] R. Buyya, R. Ranjan, R. N. Calheiros, Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities, in: 2009 International Conference on High Performance Computing Simulation, 2009, pp. 1–11. doi:10.1109/HPCSIM.2009.5192685.
[34] O. Oksiiuk, V. Chaikovska, A. Fesenko, Security technique for authentication process in the cloud environment, in: IEEE International Scientific-Practical Conference: Problems of Infocommunications Science and Technology (PIC S&T 2019) 9061248, 2019, pp. 379–382.
[35] R. S. de Carvalho, D. Saleem, Recommended Functionalities for Improving Cybersecurity of Distributed Energy Resources, 2019 Resilience Week (RWS), San Antonio, TX, USA, 2019, pp. 226–231.
[36] W. Hupp, A. Hasandka, R. S. de Carvalho, D. Saleem, Module-OT: A Hardware Security Module for Operational Technology, in: IEEE Texas Power and Energy Conference (TPEC) College Station, Texas, February, 2020, pp. 6−7.