Cloud Service for Protecting Computer Networks of Enterprises Using Intelligent Hardware and Software Devices, Based on Raspberry Pi Microcomputers

Ademi Ospanova[1*], Aizhan Zharkimbekova[2], Lazzat Kussepova[1], Aizhan Tokkuliyeva[1], Makhabbat Kokkoz[2]

[1]Department of Information Security, L. N. Gumilyov Eurasian National University, Nur-Sultan, Republic of Kazakhstan; ospanovaade@rambler.ru, lazzat_k@rambler.ru, aizhan_tok@rambler.ru

[2]Department of Information Technology and Security, Karaganda Technical University, Karaganda, Republic of Kazakhstan; aizhan_zh@rambler.ru, kokkoz_mak@rambler.ru

*Corresponding author: ospanovaade@rambler.ru

Abstract: This paper describes the development of a unified cloud service, for protecting and monitoring corporate computer networks and SOHO-class networks, with intelligent mobile software and hardware clients, based on the Raspberry Pi type microcomputer. It is planned to develop an intelligent algorithm, that performs automatic decision-making and provides recommendations, when threats are detected in the network, to finalize software and hardware, taking into account the requirements of mobility and integrability, within the cloud service. The intelligent data processing algorithm, implemented on these devices, will be based on the developed linguistic processor and the procedure of automatic assessment of network threats. Implementation of this idea consists in the development of a web service with a replenished database of threats, incidents at the nodes of a computer network and standard solutions, a system for quantitative and qualitative risk assessment, as well as, in the subsequent integration of the described intelligent mobile software and hardware device into this web application. Thus, the developed cloud service, for protecting and monitoring computer networks, will be a centralized toolkit for the joint fight against network attacks, identifying vulnerabilities in the configuration of enterprises' networks, for using and building up a database of investigated incidents and solutions, taking into account the permissible degree of data disclosure. This work presents a developed sequential plan for the implementation of this task. Attempts have been made to substantiate, theoretically, the feasibility of implementing the described task. The authors describe the relevant tools that are currently available.

Keywords: corporate networks; computer networks security; cloud service; intelligent system; single-board computer; Raspberry Pi

1 Introduction

The idea of this project naturally grew on the basis of research carried out by the authors over several years and described in works [1-4]. The results of these studies are developed examples of the effective use of Raspberry Pi microcomputers for various purposes: teaching certain disciplines [2-4], organizing a specialist's workplace including testing the security of computer networks [1-3], as well as developing fault-tolerant protected systems for information and conducting students' assessment (research in the latter direction is at the initial stages) [2]. At the same time, in the first two cases studying, selecting the components and assembling devices were carried out, taking into account the specifics of the goals pursued, as well as the corresponding software developments. The Kali Linux distribution kit is installed in the hardware and software devices for testing computer networks described in these works. The device runs a developed application for testing computer networks with a user-friendly interface and a prototype of a linguistic processor to facilitate the work of users who are not experts in the field of computer networks and do not have sufficient skills in working with Kali Linux utilities.

The next logical step in developing the concept of facilitating the task of protecting computer networks was the idea of developing a single cloud service for modern companies containing constantly available necessary tools for monitoring and protecting computer networks of enterprises, as well as a continuously replenished database of test results and monitoring networks, possible vulnerabilities, ways to eliminate them, cases of investigated incidents, decision algorithms, taking into account the permissible degree of data disclosure. At the same time, in addition to traditional software clients for cloud applications, the service includes mobile software and hardware clients with an intelligent data processing algorithm, the prototypes of which will be the Raspberry Pi-based devices described above. These devices can also be used independently of the cloud service (primarily by users who are not specialists in the field of computer network security and do not have sufficient skills in working with command line applications). In addition, the development of a flexible system of accessing these devices (SSH, a web interface integrated into a cloud service) will provide more efficient and reliable operation of this service.

Currently, the interest in cloud technologies in the world is growing due to many advantages and a wide range of opportunities provided, despite the existing disadvantages and risks at this stage. Thanks to these technologies, business organizations of various levels and trends of their activities, as well as private users, have such convenient opportunities as access to updated software tools, development tools and environments, network equipment, DBMS, hardware, consolidating and monitoring business processes, security, container technologies.

In works [5-10], some issues of cloud technologies are studied, which are indirectly included in the subject of the presented work. These are issues of ensuring network

security of enterprises (on the example of the United States) [6], provision of cloud tools for enterprises [7] [8], the use of artificial intelligence [9] and Docker technologies [10] and clustering [5].

There are such related works as corporate desktop solutions for automatic assessment of information risks according to a specific methodology with the generation of such reports as CRAMM, RiskWatch, COBRA, RA2 complexes. In the process of implementing the presented idea, it is planned to develop and to implement a system for the qualitative and quantitative assessment of vulnerabilities and risks on the nodes of a computer network related to firewall settings, access control to application ports, software vulnerabilities at workstations. This development will be required for both the web service and the smart device client. The difference between this development and the existing risk assessment methods and their implementations is in the fact that many of these methods and applications are commercial, they represent a complex toolkit for a comprehensive security assessment of the entire infrastructure of an organization, which requires large amounts of initial information. In addition, the complex development presented in this paper, among other things includes organization and algorithms of forming a renewable database of vulnerabilities, risks and investigated incidents, automation of risk assessment, which works as a part of the centralized cloud tool.

There are examples of using microcomputers of the Raspberry Pi type to control a small cloud service, the Internet of Things, and other network technologies [11-24]. However, it should be noted that to solve various problems, separate assemblies and, if needed, programming of tools are performed that meet the needs of a particular undertaking. It was noted that the authors completed those tasks to develop a device for testing security of computer networks, aiming and taking into account the specific features described in works [1-4] and including the operating system download optimizing, the response speed of the liquid crystal display, writing specialized software (for a part of which the authors' certificate was obtained), developing and implementing a prototype of the linguistic processor to facilitate the use of the device by users who are not experts in the field of computer network security or do not have sufficient skills in working with applications with a command line interface. Works [25-32] are dealing with studying the possibilities of constructing syntactic, semantic analyzers and linguistic processors including those for the Kazakh language [25], and were carried out with the aim of developing an intellectual component of question-search information systems. In this work, a formal limited language of utilities will be investigated, which in the future will allow achieving better results in the work of the morphological, syntactic and semantic components of the linguistic processor. In addition, the purpose of the development (for non-specialists) also determines specifics of the algorithm, which consists in developing a procedure of automatic evaluating the importance of utility messages, a database of interpreted messages and generating messages for the user. In addition, the development of the software part of the device will take into account small form-factors of displays to ensure mobility, as well as the issues of integrating data from smart devices as clients into the developed cloud service.

Let us note one more issue related to studying the "bare metal provisioning" technologies for creating and deploying cloud services directly to server equipment. This issue, due to specifics of the service being developed, is important for the prospects of implementing and commercializing the results obtained during implementation of the task. This issue is the subject of studies [5] [10], which consider cloud platforms that provide bare metal provisioning tools. However, works describing the process of creating and deploying cloud services directly on server hardware, container technologies, as well as describing real experience of testing with cloud service workloads [33-36], due to a lot of technical details associated with various technologies implementation and development tools used, can only serve as an approximate guide when performing similar work with a specific cloud service.

2 Methodology

Issues and expected results on the task set in the introduction can be divided into two main groups. The issues of the first group are formed sequentially from the goal of the task when planning the process of its implementation and imply mainly obtaining results experimentally.

First, this is building and deploying the model and architecture of the cloud service, the base of the subject area, the interaction of service components, infrastructure, configuration, policies for selecting the tools used that are developed at the first stage of solving the problem. For these purposes, it is necessary to develop test scenarios that take into account the possibility of clarifying and adjusting the issues and assumptions. This cloud service will have a SaaS model for most of the services provided and the infrastructure of the Community Cloud, which is caused by the purpose of the service and the prospects of its development to the concept of a single tool for protecting computer networks of enterprises.

Second, implementation of the domain semantics in the service database requires a specially developed series of tests with simulation of situations.

Third, it is necessary to answer the issues about organization and functionality of the user tools of the cloud service, taking into account the criteria of sufficiency, ease of use, performance, extensibility and upgradability, depending on new standards and specifications in the subject area.

Fourth, it is the expectation of increasing the level of computer networks security, ease of the service use due to the introduction of special intelligent software and hardware clients into the cloud service system. Through the development of an intelligent component, the device software will allow using more extensively specific tools for testing network security and taking timely protection and countermeasures. A related issue here is the confirmation of the expediency of using

the developed algorithm of intelligent processing and interpreting the limited language of specialized programs and the effectiveness of implementing this algorithm. In addition, it is necessary to obtain an assessment of the ergonomics and efficiency of the hardware and software equipment of the devices.

Fifth, there is an issue of finding the optimal scenario and tools for successful transferring a cloud service from one platform to another with different infrastructures and configurations, standards and specifications. It is also important to transfer the developed cloud system from rented cloud servers to the own servers in order to create a real model of a scalable production service, to study security issues, and to assess the labor intensity of maintenance.

The issues and expected results of the second group are solved at a more abstract level and involve theoretical research using statistical methods and forecasting. These are the issues of developing and evaluating criteria for the sustainable demand for the service. This also includes forecasting scenarios for the development and viability of the concept of the service being developed as a single centralized toolkit for protecting computer networks, determining and evaluating future prospects, conclusions and opportunities for commercialization. Using the evidence base and justifications obtained when considering the first group of issues will allow you obtaining more accurate estimates and decisions for this group.

In the process of implementing the task, the following *types of experimental work* are sequentially performed:

1) Testing against various criteria of tools and development environments in order to eliminate errors in scalability, updating and reliability of the service.
2) Verifying the base of vulnerabilities and the developed quantitative and qualitative system for assessing risks and vulnerabilities.
3) Verifying compliance of the developed database architecture with the tasks of the service, selection of methods and means of protecting cloud services and testing in various scenarios.
4) Determining authority and available functionality of service accounts.
5) Testing the service under loads to improve performance and debugging.
6) Iterative prototyping of a linguistic processor for an intelligent computer network testing system.
7) Testing and evaluating the effectiveness of the database of interpreted messages of the utilities for monitoring and testing computer networks.
8) Implementing, testing and evaluating the complexity of the algorithm of intelligent processing of a formal program language.
9) Assembling with various configurations and upgrading the hardware and software device (based on Raspberry Pi) in order to improve ergonomics and convenience for performing the required tasks.

10) Testing the developed layouts of generated documentation (reports on network security checks, recommendations).
11) Testing according to various criteria of the device as a client of the developed service.
12) Creating test scripts and complex testing with workloads of the cloud service and related developments.
13) Working with container technologies and working out the process of transferring the service to other servers in order to model a real scalable production service in the premise for the subsequent commercialization of the project results.
14) Organizing a cluster of servers, installation and configuration of the working environment, the necessary peripheral devices. Checking performance.

The description of the stages of solving the problem is given in Table 1, where the above types of experimental work are also correlated with these stages. The sequence of the steps is shown in Figure 1.

Table 1

Stages of implementing the cloud service and types of experimental work

Stage	**Description of the problem solving stage**
Types of work	
1	The modeling of the final cloud service is being performed, as well as a detailed plan of future developments.
1, 3, 4	
2	The main information content of the service for enterprises is being developed. The subject base is a useful convenient single source of up-to-date information for enterprises registered in the cloud system.
2	
3	This stage is a subtask of developing and launching a unified cloud service. This is developing the necessary technical components of the service including the client part, as well as documenting all possible procedures for using the service functionality by the client, assessing the security of the service and testing. This stage is a logical continuation of stages 1-2, as well as the completion of developing a cloud service as an information source.
5	
4	One of the important stages of solving the problem. It is planned to develop a new algorithm for intelligent processing the language of specialized utilities for protecting and monitoring the networks. It will be necessary to create a morphological analyzer (parser) and a message parser. It will also be necessary to develop and to implement an algorithm of automatic determining the level of danger from the messages of the utilities. Finally, based on the solutions to the above subtasks, an algorithm will be developed and implemented that will allow monitoring and testing the

6, 7, 8	networks in a regular mode for people who do not have sufficient knowledge in the field of network security, as well as people who do not have skills to work with specialized software. The program will provide results and recommendations in an adapted language that non-specialist users can understand.
5 *9, 10, 11*	This stage is necessary for logical completion of the results obtained at stage 4. The device with an intelligent program for testing and consulting non-specialist users will be optimized in software and hardware in order to improve its usability.
6	The logical continuation of stage 5. Namely, the hardware and software device for intelligent network testing developed at stages 4-5 is planned to be integrated into the cloud service developed at stages 1-3. As a result, the cloud service will turn from an information source into a full-fledged single centralized interactive tool for protecting networks with a replenished up-to-date vulnerability base, a history of testing by the bank of solutions. The use of the tool will be possible both through the classic client application implemented in stage 3 and through the smart device developed in stages 4-5.
7	The stage will provide an even more convenient use of the smart device system and cloud service. A module for managing an intelligent mobile device will be developed and integrated into the service created at stages 3-6.
8 *12*	The resulting stage of the previous subtasks; testing work with real workloads is carried out here, complete supporting documentation is formed.
9 *13, 14*	Stage 9 is an important subtask for modeling a real unified cloud service running on a specially created local server cluster. The subtask is performed with the aim of researching and predicting the conditions for the successful implementation of the service concept as a single centralized tool for joint protection against cyber threats. The research will also formulate practical instructions for using the technologies of transferring services to other servers.

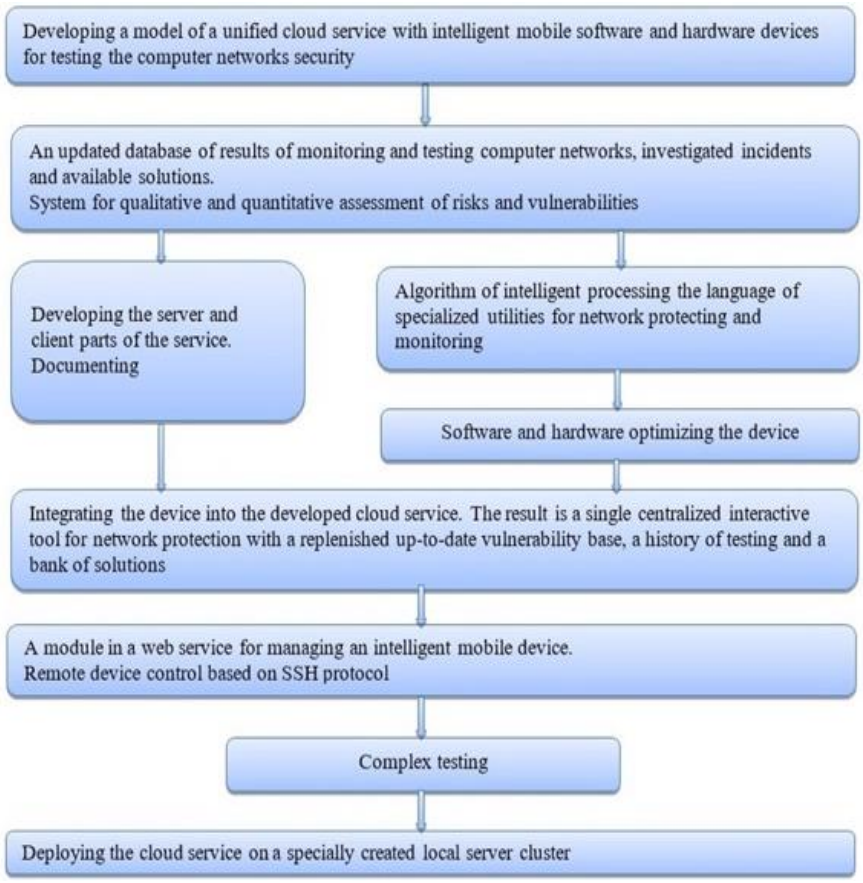

Figure 1
Sequence of realizing the tasks of the cloud service construction and deployment

3 Results and Discussion

Below there are some solutions for the successful implementation of the task of constructing the described unified cloud service. Some criteria of considering cloud platforms for long-term performance are presented in Table 2.

It should be noted that the data and technologies presented in Table 2 are applicable only for creating and testing a model of the developed cloud service, while the specifics of the concept implies the organization of a private, independent cloud infrastructure.

Table 2
Possibilities of using cloud providers to create a unified cloud service model for protecting computer networks of enterprises

Criterion	**Explanations**
Vendor policies and standards	Studying the offered service packages, contract terms, prices, level of support. Investigate the issue of the vendor lock-in. It is necessary to study examples of best practices for deploying and maintaining cloud services, taking into account the differences in the terminology used
The service volume, the technologies used	IaaS virtual infrastructure, IT-outsourcing ITaaS, data backup and recovery, special software (databases, 1C), protection against DDoS attacks, data protection using hardware solutions, encryption. Hypervisors and other virtualization solutions used. Manufacturers, specifications, service and timely replacement of equipment. Disaster recovery, fault tolerance technologies
Supporting various cloud models and infrastructures	Use of promising and flexible Docker technologies, service modernizing and transferring technologies. Scalability, bi-directional migrations. Provided level of control and related tools.

Figures 2 and 3 show respectively a general and a schematic diagram of the cloud service corresponding to a SaaS model with a Community Cloud infrastructure. To build a service model and test its main functionality, it is required to use IaaS (Infrastructure as a Service) of one vendor that meets the conditions specified in Table 2.

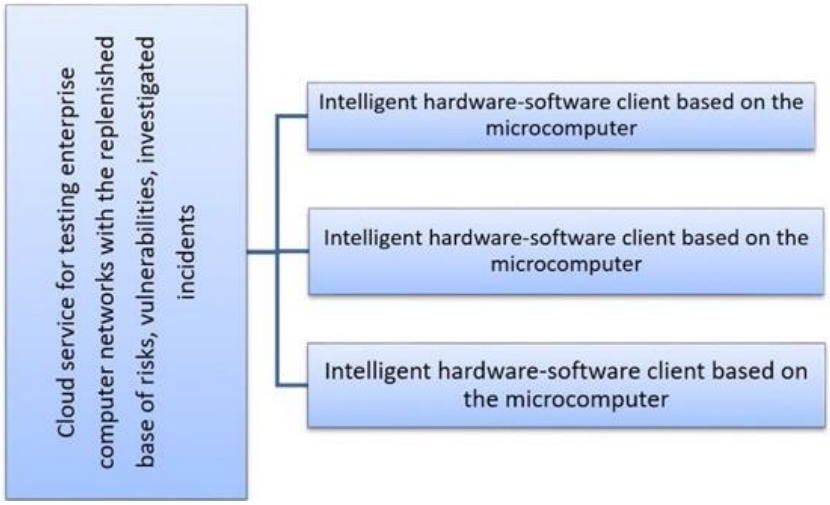

Figure 2
General diagram of the service with software-hardware clients

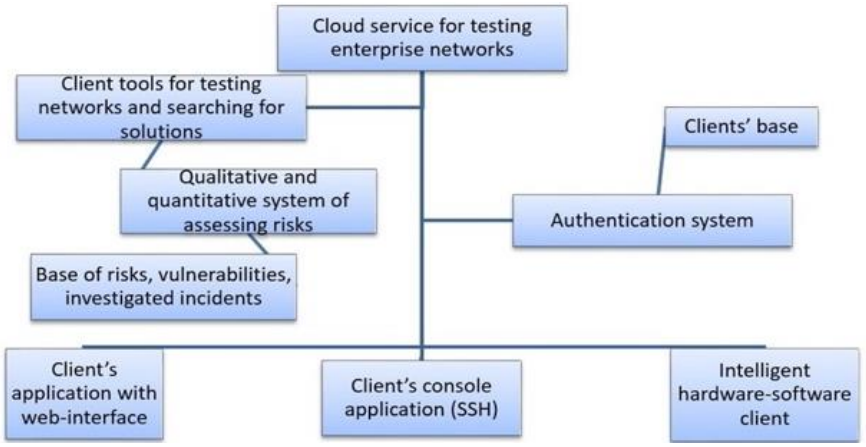

Figure 3
Principal diagram of a single cloud service for protecting computer networks of enterprises

The requirement to support flexible scalability, as well as rather narrow specialization of the service database give grounds for selecting a document-oriented DBMS such as MongoDB and creating a NoSQL database. A cloud service (SaaS) training example developed by the authors on the Heroku cloud platform (PaaS) ([37]), using one of the Heroku stacks with a GCC compiler, explored the capabilities of this cloud provider. In addition, the new ability to leverage the ObjectRocket for MongoDB on Heroku will allow developing functional requirements for the web application and service clients.

Selecting configurations, infrastructures and security of computer networks in the case of modeling this service and use by a limited community is determined based on the analysis of cloud providers according to the criteria given in Table 2. In the case of creating a single service to protect computer networks of a significant number of enterprises in the country, which is the task of the last stage of implementing the presented idea, these issues are considered on the basis of marketing, economic and other research obtained with this specific data and calculations for them.

Let's talk about the solution of the problem 2) in more detail (solutions to other problems are subject of our next work). It is being formed a database of vulnerabilities and risks on the nodes of a computer network, as well as to create a quantitative and qualitative risk assessment system that will operate on the service and in the software part of the client device. The criteria for the risk and vulnerability assessment system were based on the recommendations of the standards "ISO / IEC 27005: 2018 Information technology - Security techniques - Information security risk management", "BS 7799-3: 2017 Information security management systems. Guidelines for information security risk management", as well as document [38]. For example, in the criterion for assessing the probability of threats to a critical asset for assessing information risks at enterprises the parameters

were included X_{own}, X_{common}, D_k, where X_{own} is frequency of realization of information security threat to a critical information asset for a certain past period, X_{common} is similar statistics on other organizations, D_k defines criterion of the complexity of the threat. The value of an arbitrary criterion C_i for assessing information risks is determined by a number of parameters $P_j (C_i = \sum_j^n = 1 P_j)$. Then these parameters are taken into account in the assessment as follows:

$$R = \sum_{i=1}^{k} (\prod_{j=1}^{n} P_j)\, k_1 X_{own} k_2 X_{common} D_k$$

where $0 < k_1, k_2 \leq 2$. The parameter D_k is determined for a specific enterprise on the basis of statistical data and probabilistic estimates, taking into account the practical feasibility coefficient k. Note that, in comparison with the results of applying some known methods for assessing information security, the use of these parameters in the given way gives varying results (the variation is due to the use of non-constant coefficients of type k).

Remark. The condition $1 > k_1, k_2$ means that there is a decrease in the number of the studied cyber-attack type; if $k_1, k_2 \geq 1$ then it is possible to predict an increase in the probability of cyber-attacks and dynamically take this coefficient into account to refine estimates.

Modelling situations and states of nodes of a computer network can be based on studying the educational networks deployed in the Internet that are intended among other things for their testing, known data of application ports, firewall settings, software vulnerabilities, network protocols.

Selecting the main testing criteria at all stages of development (software, models, procedures) determines test scenarios including those with different quantitative characteristics of workloads. Testing the service for workloads includes testing using special software, and for certain parts it is planned to create scripts that reproduce the behavior of both real users and attackers. Some criteria for testing cloud services, risk and vulnerability assessment systems, and the intelligent part of the device are described in Table 3.

Table 3

Data for testing developments at various stages of the task

Type of task	**Criteria of testing and explanations**
1. The service model and architecture	Checking the selected tasks at the levels of business logic (subject area) and user interaction (including taking into account software and hardware smart clients) by the method of hierarchical decomposition. Verification of the selected infrastructure, taking into account support capabilities, scalability, portability, upgradeability, security. Checking the integrity, logical independence of the designed modules. Generation of diagrams of the use, classes, interactions and generation of code templates

2. The system of assessing risks and vulnerabilities	Checking the completeness and consistency of the identified network threats, vulnerabilities and attack scenarios based on regulatory documents and collections of best practices. Comparison of the scale and method of assessment developed on the basis of existing standards and statistical studies with the results of known risk assessment methods
3. Web-service	Verification of support capabilities, scalability, portability, upgradability, security subsystem, demilitarized zone, RAID technologies, module integrability. Loads by emulating use cases, as well as using special testing tools (WebLOAD, StresStimulus) to check the sensitivity of the web service to requests and their number, the speed of request processing, the impact of channel bandwidth, fault tolerance, and recovery time after a failure. Checking the sufficiency and convenience of client tools (for example, using the method of expert assessments, fuzzy algorithms).
4. Intelligent system	Checking the adequacy of interpreted messages and recommendations generated on the basis of the developed system for assessing threats, vulnerabilities and attack scenarios based on existing classifications of the hazard level, as well as using the method of expert assessments. Checking the work of the linguistic processor by specifying a variety of query options. Checking the running time and comparing it with the theoretical difficulty estimate.
5. Hardware-software device	Verification of thermal characteristics and local power supply, comparison with nominal characteristics. Checking the adaptability of the application to the displays used. Checking the loading speed and stability of work for different types of flash cards and different window managers. Checking the efficiency of the displays in different modes and optimizing the load using the developed scripts, finding out the dependence of the operating time on the battery capacity. Checking RAM with the use of special utilities.
6. Intelligent hardware-software client	In addition to the criteria specified for the previous type of task, checking the stability and speed of the interface with the web service; the speed of updating the database of the subject area; device operation via SSH protocol: remote access to the device; checking the device's network interface (wireless and wired).
7. Single cloud service with software-hardware clients	Verification, according to specially created testing scenarios that include the criteria highlighted in tasks 1-6 of this table. Checking the selected container method: all the functionality of the portable service, update capabilities, scalability. Taking into account the obtained results, deploying the service model on a local server cluster and testing according to the same scenarios.

For the effective functioning of the service, procedures are created for using a web application, a hardware and software device. User action scenarios represent possible options for using the client tools implemented on the cloud service, the

functionality of the hardware and software device, interpreting the results, as well as a description of further actions. Algorithmization of the service creation process is carried out in order to obtain the possibility of deploying the service on server infrastructures of various configurations. For this purpose, specially developed scripts are used: to check the characteristics and physical parameters of equipment, capacities of physical media, communication channel width, to set user quotas, for testing.

In addition, one of the main tasks involves the use of artificial intelligence methods, in particular, constructing a linguistic processor, developing a database of interpreted messages in the construction and implementing the algorithm of intelligent data processing. This algorithm will operate on the device which prototype is shown in Figure 4.

Within the framework of optimizing the device in terms of hardware, in view of the aim of creating a portable device, it seems appropriate to take into the development displays with the diagonal of 3.2 " and 5 " (of higher resolution than shown in Figure 4). For the same purpose, it is planned to optimize the built-in power supply in terms of capacitive parameters (a 2500 mAh lithium battery is built into the device in Figure 4). These displays require a special graphical user interface of the developed intelligent program. Due to a more powerful processor and an increased amount of RAM up to 8 GB, the Raspberry Pi Model 4B microcomputers show worse thermal performance than the Raspberry Pi 3B+, which is used in the project and provides all the needs.

Figure 4
A prototype of a portable hardware-software client of the developed cloud service

Regarding the last stage of implementing the presented idea, it is planned to test container technologies and the completed development on a specially created local cluster of servers. The purpose and the description of the experimental and

theoretical results at this stage are given in Table 1. This experimental work is planned to be carried out on existing servers with the characteristics described in Table 4. The infrastructure configuration will correspond to one of the typical options with the allocation of a demilitarized zone and installation of a middle-class hardware firewall of the CiscoFirepower 1010 NGFW Appliance type.

Table 4
Characteristics of the cluster servers

Two servers HP ML150 G6, 2xQuad-Core Xeon E5540 2.53 GHz 8 MB L3 Cache 192 GB RAM 1TB HDD DVD-RW
One server HP Enterprise ML350 Gen10/1x Intel Xeon Silver 4110 2,1GHz 11 MB Cache 64 GB RAM 5 TB HDD

Statistical studies of attacks on enterprise networks (the growth of their number, the focus and level of danger), software and hardware vulnerabilities (detection tools, dynamics, implementation possibilities, damage level) will be carried out, taking into account the types of enterprises and their activities over the past two decades.

In work [39] a forecasting method based on the use of time series is given. The authors have at their disposal implementation of this algorithm in the Fortran language, which has been successfully tested on multifactor data. This implementation is planned to be used to predict the effectiveness, feasibility, viability, development prospects of the developed cloud service. The initial data in this task will be the data obtained in the course of the above-described statistical study.

In the present day world of "informatization" and digitalization, such problems as developing cloud technologies, solving cyber security problems, increasing the level of digital literacy and awareness of the degree of danger and scale of cyber threats are really relevant, global and determine the needs of both the enterprise and the state level. In various countries of the world, long-term and short-term programs of developing and strengthening protection of national cyberspace are continuously being developed and implemented. Preventive measures to ensure information security, technologies of analysis, investigation and protection are functioning and are being improved. For example, in Kazakhstan, the Cyber Security Concept ("Cyber Shield of Kazakhstan") [40] and the State Program "Digital Kazakhstan" [41] are in force. Developing a unified cloud service model for protecting Corporate Networks and SOHO class networks with a replenished database of vulnerabilities, threats, incidents and solutions fully meets the identified problems.

The presence of intelligent mobile hardware and software clients in the service being developed, which are convenient for non-specialists in the field of computer network security, will advance in solving the problems of increasing digital literacy

and awareness of the degree of danger and scale of cyber threats. Finally, the potential danger and obvious destructive power of cybercrimes and cyber warfare makes it appropriate and necessary to consider the possibilities of deploying this cloud service using the "bare metal provisioning" technology on separate servers with the Community Cloud infrastructure to create a single independent hardware-cloud package for protecting computer networks.

Let us note the interest of Kazakhstan companies, in the developed a unified cloud service, for monitoring and protecting computer networks: Letters of interest were received from a number of companies.

Conclusions

In this paper, the research and practical work performed by the authors is presented. The idea of creating a unified cloud service, for the protection and monitoring of corporate computer networks and SOHO class networks, with intelligent mobile software and hardware clients based on microcomputers of the Raspberry Pi type, is presented, the corresponding problems are also formulated. A review of the current research and related research topics was carried out. The theoretical substantiation of the feasibility of the described task, has been also been presented. The authors' current groundwork for this study is described.

Herein, is the presentation of the developed plan for implementing the task with a full description of the stages of implementation. The authors' developments: A training example of a cloud service (SaaS) on the Heroku platform (PaaS) ([37]), which uses one of the Heroku stacks, with a GCC compiler, as well as, projects [42-44] deployed there, have made it possible to explore the possibilities provided by the cloud provider Heroku, which will be the main work of the authors in stage 3 of the problems presented in this work.

The full implementation of this task will provide a clear, theoretical and experimental substantiation, of the feasibility and technical capabilities, of creating an effective cloud service, for protecting computer networks, with clients based on the Raspberry Pi microcomputer. In addition, the results obtained will provide experimental confirmation of the possibility of developing a scalable production service. As a consequence, the results will also allow predicting qualitative and quantitative assessments of the possibility of their commercialization, with potential consumers, both in the form of Associations of Business communities (B2B business model) and at the State level (B2G business model).

Acknowledgement

This research is funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP09561712).

References

[1] A. B. Ospanova, B. R. Sauanov, "Network security tools based on the Raspberry Pi microcomputer," Proceedings of the IV International

Scientific-Practical Conference "Intelligent Information and Communication Technologies - A Means of Implementing the Third Industrial Revolution in the Light of the Strategy “Kazakhstan-2050”. L. N. Gumilyov Eurasian National University, Nur-Sultan, 2017, pp. 380-382

[2] A. B. Ospanova, B. I. Tuleuov, “Prospects for using the Raspberry Pi microcomputer in effective digitalization of Kazakhstan,” Bulletin of ENU n.a. L.N. Gumilyov. Series “Mathematics. Computer Science. Mechanics”, Vol. 4, No. 125, pp. 95-107, 2018

[3] A. B. Ospanova, G. Ualikhanov, A. T. Zharkimbekova, “Management of Kali Linux utilities,” IX International Scientific and Practical Conference of Young Scientists “Education, Science, Innovation - the Contribution of Young Researchers”. L. N. Gumilyov Eurasian National University, Nur-Sultan, 2018, pp. 336-339

[4] A. Zharkimbekova, A. Ospanova, K. Sagindykov, M. Kokkoz, “Implementation and commercialization of the results of the “multidisciplinary mobile computer classroom based on Raspberry Pi” project,” International Journal of Emerging Technologies in Learning, Vol. 15, No. 13, pp. 116-135, 2020

[5] U. S. Patki, “Clustering algorithms and their applications in cloud computing environment,” International Research Journal of Computer Science, Vol. 4, No. 04, pp. 14-16, 2017

[6] C. L. Gorham, “Developing enterprise cyber situational awareness,” International Journal of Managing Information Technology, Vol. 12, No. 3, pp. 1-8, 2020

[7] S. K. Ravichandran, A. Sasi, “Effective storage of goods in a warehouse using farm optimization algorithm,” International Journal of Cloud Computing, Vol. 9, No. 2-3, pp. 207-215, 2020

[8] M. Attaran, J. Woods, “Cloud computing technology: improving small business performance using the Internet,” Journal of Small Business & Entrepreneurship, Vol. 31, No. 6, pp. 495-519, 2019

[9] Y. Hu, H. Wang, W. Ma, “Intelligent cloud workflow management and scheduling method for big data applications,” Journal of Cloud Computing, Vol. 9, No. 39, pp. 39-52, 2020

[10] A. Ahmed, G. Pierre, “Docker-pi: docker container deployment in fog computing infrastructures,” International Journal of Cloud Computing, Vol. 9, No. 1, pp. 6-27, 2020

[11] The MsgPi, Raspberry Pi Projects Book, 5th ed., Seymour Distribution Ltd., London, 2020, https://magpi.raspberrypi.org/books/projects-5/pdf

[12] The MsgPi, "Essentials – conquer the command line," 2nd ed., Seymour Distribution Ltd., London, 2019, https://magpi.raspberrypi.org/books/command-line-second-edition/pdf

[13] J. F. Nusairat, Rust for the IoT: Building Internet of Things Apps With Rust and Raspberry Pi, Apress, New York, 2020

[14] C. Berg, Raspberry Pi 4 For Beginners and Intermediates: A Comprehensive Guide for Beginner and Intermediates to Master the New Raspberry Pi 4 and Set up Innovative Projects, Independently Published, Traverse City, 2020

[15] W. Rahman, E. Hossain, R. Islam et al., "Real-time and low-cost IoT based farming using raspberry Pi," Indonesian Journal of Electrical Engineering and Computer Science, Vol. 17, No. 1, pp. 197-204, 2020

[16] K. N. Myint, M. H. Zaw, W. T. Aung, "Parallel and distributed computing using MPI on Raspberry Pi Cluster," International Journal of Future Computer and Communication, Vol. 9, No 1, pp. 18-22, 2020

[17] J. Schlobohm, A. Pösch, E. Reithmeier, "Raspberry Pi based portable endoscopic 3D measurement system," Electronics, Vol. 5, No. 3, pp. 43-51, 2016

[18] W. Gay, Custom Raspberry Pi Interfaces: Design and Build Hardware Interfaces for the Raspberry Pi, Apress, St. Catharines, Ontario, Canada, 2017

[19] S. Monk, Cookbook by Raspberry Pi, O'Reilly, United States of America, 2016

[20] M. E. Soper, Expanding Your Raspberry Pi: Storage, Printing, Peripherals, and Network Connections for Your Raspberry Pi, Apress, Indianapolis (Indiana, USA), 2017

[21] V. Tzivaras, Raspberry Pi Zero W Wireless Projects, Packt Publishing, Birmingham-Mumbai, 2017

[22] M. Schwartz, Building Smart Homes With Raspberry Pi Zero, Packt Publishing, Birmingham-Mumbai, 2016

[23] S. Chin, J. Weaver, Raspberry Pi With Java. Programming the Internet of Things (IoT), Packt Publishing, Birmingham-Mumbai, 2016

[24] "Raspberry Pi Foundation: Temporary failure in name resolution," 2019, https://www.raspberrypi.org/forums/viewtopic.php?t=157047&p=1023463

[25] V. B. Barakhnin, L. Kh. Lukpanova, A. A. Solovyev, "Algorithm for constructing word forms using inflectional classes for systems of morphological analysis of the Kazakh language," Vestnik Novosibirsk State University Series: Information Technology, Vol. 12, pp. 25-32, 2014

[26] J. Su, V. Vysotska, A. Sachenko, V. Lytvyn, Y. Burov, "Information resources processing using linguistic analysis of textual content," 2017 9th

IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). IEEE, Piscataway, 2017, pp. 573-578

[27] K. J. Lyytinen, "Implications of theories of language for information systems," MIS Quarterly, Vol. 9, No. 1, pp. 61-74, 1985

[28] A. M. Andreyev, D. V. Berezkin, and A. V. Brik, "Linguistic processor for information retrieval system," n.d., http://www.inteltec.ru/publish/articles/textan/art_21br.shtml

[29] S. V. Kolosov, "Linguistic processor in the Internet smart search system," Bulletin of the Altai State Technical University I. I. Polzunov, Vol. 2, pp. 169-172, 2014

[30] T. G. Skrebtsova, A. Klementyeva, S. Kuznetsov, S. Suvorov, Linguistic Analyzer, Converting Text to a Meta-Language Data Structure, Publishing House of St. Petersburg University, Saint Petersburg, 2019

[31] V. V. Garshina, Yu. A. Bogoyavlenskaya, "Development of a linguistic parser for the Russian language," Vestnik VSU, Series: System Analysis and Information Technology, Vol. 2, pp. 174-182, 2012

[32] N. I. Gurin, Ya. A. Zhuk, "Morphological analysis of the text for generating the knowledge base of the dialogue information system," Proceedings of Belarusian State Technological University, Vol. 6, pp. 156-159, 2016

[33] L. J. M. Nieuwenhuis, M. L. Ehrenhard, L. Prause, "The shift to Cloud Computing: the impact of disruptive technology on the enterprise software business ecosystem," Technological Forecasting and Social Change, Vol. 129, pp. 308-313, 2017

[34] I. V. Bogomolov, A. V. Aleksiyants, O. D. Borissenko, A. I. Avetisyan, "Problems of scalability of cloud environments and the search for the causes of degradation of the central identification service Openstack Keystone," Izvestia SFedU: Engineering Science, Vol. 12, pp. 130-140, 2016

[35] E. L. Aksenova, V. V. Shvetsova, O. D. Borisenko, I. V. Bogomolov, "Implementation of a service to replace Keystone as the central identity service of the Openstack cloud platform," Proceedings of ISP RAS, Vol. 29, pp. 203-212, 2017

[36] Z. Li, C. Yan, X. Yu, N. Yu, "Bayesian network-based virtual machines consolidation method," Future Generation Computer Systems, Vol. 69, pp. 75-87, 2017

[37] A cloud service (SaaS) training example, n.d., http://afd-2.herokuapp.com

[38] Resolution of the Board of the Agency of the Republic of Kazakhstan for the Regulation and Development of the Financial Market, No. 111 dated November 23, 2020 "On approval of the methodology for assessing information security risks, including the procedure for ranking financial

organizations according to the degree of exposure to information security risks", http://adilet.zan.kz/rus/docs/V2000021686

[39] M. Otelbayev, M. A. Sadybekov, B. I. Tuleuov, "Integral model and forecasting of vector dynamic series of economic parameters," International Journal of Pure and Applied Mathematics, Vol. 113, No. 4, pp. 125-138, 2017

[40] Ministry of Justice of the Republic of Kazakhstan, "Cyber Security Concept ("Cyber Shield of Kazakhstan")," 2017, http://adilet.zan.kz/rus/docs/P1700000407#z15

[41] "Digital Kazakhstan State program "Digital Kazakhstan", 2017, https://digitalkz.kz/

[42] Electronic digital signature (EDS), n.d., crypt-esign.herokuapp.com/

[43] Decision Making under Uncertainty, n.d., dmuu.herokuapp.com

[44] Cryptanalysis by Software Means, n.d., ca-enu.herokuapp.com