An intelligently distributed system for controlling information flows

Irina Zhuzhgina[1] and *Alexey* Lazarev[1*]

[1]Department of Information Technology in Economics and Management, branch of the National Research University 'Moscow Power Engineering Institute' in Smolensk, Energy passage 1, 214013 Smolensk, Russia

Abstract. The existing controlling software toolkit is represented by multiple software modules to ensure effective organizations management. An important most information systems component is the possibility of remote and distributed work in multi-user mode. At the same time, the disadvantages of multi-level TCP/IP routing, the presence of various CVE vulnerabilities contribute to data leakage and unauthorized changes. Based on these conclusions, the main purpose of the study can be identified – the development of an intelligently distributed traffic tunnelling system. The proposed approach uses deep learning models both for predicting IP address samples during initialization of a secure connection and for dynamic network traffic filtering in the DNS server. The proposed authentication algorithm based on the dynamic extension of the function made it possible to automate the trusted client's authorization process, and the implementation of a combined decision–making system - to ensure the correct interaction of all software modules. The development result of the proposed system allowed both to reduce time costs when working with controlling information systems and to ensure safe interaction.

1 Introduction

At the moment, controlling is an modern business integral part and one of the most important areas in the business management practise, as it allows to ensure the effectiveness and sustainability of the organisation's development [1]. Considering its structure, the following elements can be distinguished:

- financial (planning, management and control of business financial aspects, such as budgeting, credit and investment management, accounting and reporting);
- operational (planning, management and control of operational processes in the organisation, such as production, logistics, procurement, etc);
- strategic (planning, management and control of business strategic aspects, such as strategy development, market and competitor analysis, new products and services development);
- controlling information flows (planning, management and control of the information flows implementation in the organisation, such as database management, information security);

---

* Corresponding author: anonymous.prodject@gmail.com

• personnel controlling (planning, management and control of the organisation's staffing, such as recruitment and hiring, training and development of employees, evaluation and motivation).

Each of these controlling elements is interrelated and important. Moreover, these elements can be expanded (supplemented) with other components, depending on the specific goals of the organisation.

At the same time, at the moment, among all application of controlling areas and its functional areas, information flows controlling has become the most widespread, as well as visible significant practical results for organisations. The following information flow controlling tools can be distinguished that allow automating a number of business processes in an organisation: SAP Business Objects Planning and Consolidation, 1C:ERP Enterprise Management 2 ("1C:ERP UP 2"), IBM Cognos Controller, Oracle Hyperion Financial Management, Anaplan, Adaptive Insights, Prophix [2]. These tools provide financial planning, budgeting and data processing capabilities. At the same time, for example, 1C:ERP UP 2 provides ample opportunities for remote administration and work with individual data – 1C can be singled out as priority solutions: Link, 1C-Connect [3]. These tools provide the end user with the ability to work with a remote server via a web interface, while providing additional features in the form of encryption using TLS, AES + RSA, HTTPS, and embedded electronic signature certificates.

Among the disadvantages of these solutions, one can single out the need to purchase certain solutions, or the need to adapt the 1C:ERP UP 2 server to the requirements of 1C:Link, 1C-Connect. An alternative approach to implementing remote access without purchasing additional licences is the process of connecting to a remote server via an IPv4/IPv6 address, or using Remote Desktop Protocol (RDP) in remote application mode [4-5].

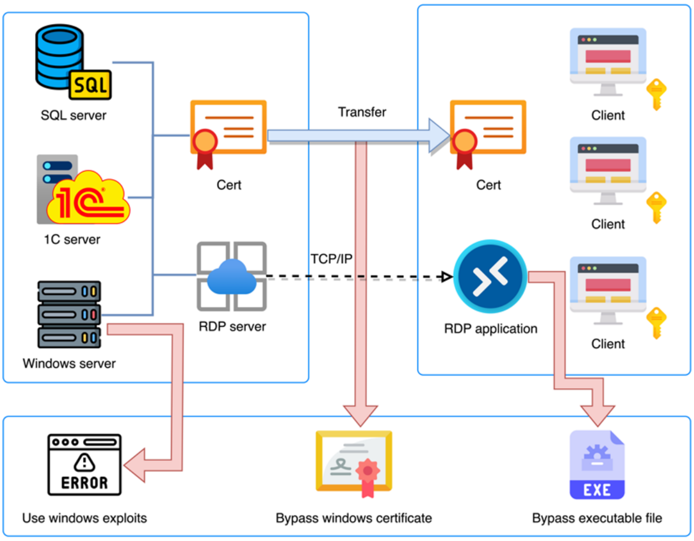


Fig. 1. Example of connecting to 1C using RDP / RemoteApp

As can see from Fig. 1, the process of connecting to the 1C server via the RDP App works through the application layer (7) of the TCP/IP protocol using a self-signed server certificate.

The OSI channel layer, in turn, is responsible for routing data within a local network segment with support for IEEE 802.2, 802.3 standards with channel management and frame traffic functionality [6]. The disadvantages of the OSI network layer (3) in the topology under consideration are the problems of IP address assignments duplication of DHCP server, as well as significant problems of conducting massive DDOS attacks – denial of service is possible when conducting such attacks on target services, however, by default, a TCP connexion involves allocating a limit on the waiting time for a response [7]. At the same time, in the process of its operation, a vulnerabilities number can be identified both at the level of the server / client operating system, and when transferring the certificate, as well as the injecting malicious code possibility into the target application. For example, BlueKeep Exploit (CVE-2019-0708), implemented in 2019, currently allows to use Refresh Rect PDU, Bitmap Cache (PDU) data blocks to make changes to the core of Microsoft Windows operating systems, the result of which provides access to an administrative account without authentication [8].

As a result, can say that the existing software tools use, of course, allows to solve the task, but the presence of a problems number in their practical use based on TCP/IP protocols and the Microsoft Windows operating systems functionality does not provide an adequate security level for processing confidential data in the 1C:ERP UP 2 application. This only confirms the relevance of the traffic distribution problem between application clients when managing a modern organisation. To overcome it, an intelligently controlling information flows distributed system is proposed, the description of which is presented in this paper. The provided solution covers the ensuring secure data transmission issues in the conditions of using outdated and potentially vulnerable versions of protocols and various software prone to leaks of confidential data.

At the moment, when building various TCP/IP topologies, it is possible to distinguish two types of networks – centralised and decentralised (distributed). The centralised approach assumes the use of a file-server topology, in which all information is processed on a fixed network node (server subnet), while the distributed management approach assumes the possibility of data processing on multiple client computers. The implementation of the latter approach allows for data redundancy due to the formation of several connexions between servers, as well as the possibility of implementing a flexible approach in companies with outsourcing hiring of employees.

In general, an intelligently distributed system of controlling information flows is a closely interrelated number set of information movements about elements spaced in space, each of which does not depend on the others, but interacts with them to perform a common task and which can be aggregated into the following functional blocks:

- initialising a secure connexion between individual organisations;
- distribution and traffic redistribution of information flows between the system participants;
- client authentication;
- decision support system for managing the distribution of information flows.

A distinctive feature of this system is the ability to distribute traffic using a flexible packet routing topology and authentication based on deep network models.

2 Implementation of a secure interaction system

2.1 Structure development of the secure connexion initialization protocol between individual organisations

Most distribution topologies of client access to the processing server are carried out using the usual address distribution topology via a DHCP server, and as additional features – the priority billing use of users based on Quality of Service (QoS) [9]. In the administrative management topology case of an organisation with multiple branches, the distribution topology of administrative points can be separated by subnets. The proposed approach to the implementation of a secure controlled connexion is proposed to use the following structure at the OSI transport layer, shown in Fig. 2.

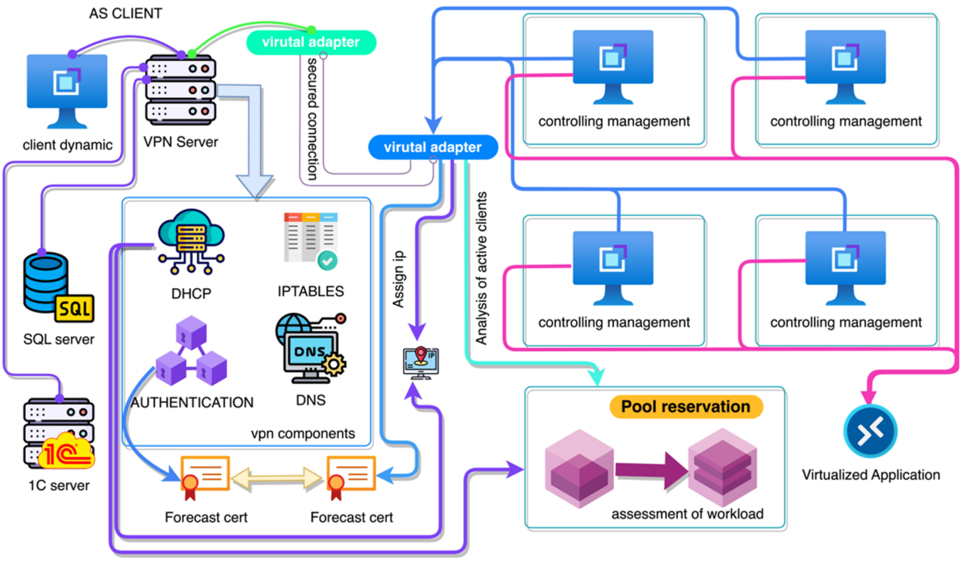


Fig. 2. Client-server topology of devices TCP/IP interaction based on the OSI transport layer

As can be seen from the Fig. 2, a multi-module system for building a secure topology consists of VPN server modules DHCP server, AUTH server, DNS server, as well as a set of configured IPTABLES tables. The main interaction in the proposed topology is carried out using the remote application port based on the Internet connexion isolation. Among other things, this topology has the ability to dynamically generate and exchange certificates to provide additional security.

The DHCP server, which is a priority module in the secure connexion initialization server, is a proprietary *dhcpd* service that provides clients with a specified set of IP addresses [10]. By default, the deployment of the address distribution server is fixed according to the principle described in Listing 1, however, in this interpretation, the main distribution of the *dhcpd* server is a trained neural network model based on a specific pool of IP addresses.

```
# Listing 1. DHCP Base configuration subnet 8.1.1.0 netmask 255.255.255.0 {
range 8.1.1.5 8.1.1.254;
option domain-name-servers 8.1.1.1;
option routers 8.1.1.1;
}
host dhc-1 {
hardware ethernet f4:e2:e8:73:a6:55; fixed-address 8.1.1.10;
}
host dhc-2 {
hardware ethernet bf:4f:83:ae:be:f9; fixed-address 8.1.1.11;
option routers 8.1.1.1;
}
```

As can see from the presented Listing 1, *8.1.1.0* is used as the main network, indicating the main DNS server. Among other things, the specified implementation allows to assign a static address for a specific MAC address, as specified for dhc hosts 1, 2. In cases of OpenVPN / WireGuard servers implementation, the configuration of the allocated pool is carried out through virtual bridge interfaces for the destination *ipaddr* server and traffic transmission via the tap interface (*modprop / brct aadif*). In this case, the binding process is carried out according to Listing 2.

```
# Listing 2. DHCP Routing # proprietary dhcp server
subnet 8.1.1.0 netmask 255.255.255.0 {
range 8.1.1.5 8.1.1.254;
option routers 8.1.1.1;
option broadcast-address 8.1.1.255;
option subnet-mask 255.255.255.0;
option domain-name-servers 8.1.1.1; option ip-forwarding on;
next-server 8.1.1.1;

option ms-classless-static-routes 24, 1,1,1, 8,1,1,1,
24, 2,2,2, 8,1,1,1,
24, 8,1,10, 8,1,1,1;}
# client configuration
...
route 0.0.0.0 8.0.0.0 net_gateway
route 64.0.0.0 8.0.0.0 net_gateway
route 128.0.0.0 8.0.0.0 net_gateway
route 8.0.0.0 8.0.0.0 net_gateway
# disable default route
#route-gateway 127.0.0.1
```

According to Listing 2, the process of using an external DHCP server is tied to the use of non-standard routes that define a third-party server as an internal one. A secondary point necessary for the implementation of minimal VPN server operation is the setting of iptables rules that allow redirecting, accepting or rejecting packets on a given interface [11]. An example of the software implementation of this module is shown in Listing 3.

```
# Listing 3. Example of setting up redirection rules if self.input_peer:
if conf.vpn. iptables and INET_TABLES: rule = self._init_rule() rule.in_interface =
self.ext_interface rule.dst = self.ext_network rule.create_target(’ACCEPT’)
self._accept.append((’INPUT’, rule)) else:
self._accept.append([ ’INPUT’,
’-i’, self.ext_interface, ’-d’, self.ext_network, ’-j’, ’ACCEPT’,
])
```

Listing 3 demonstrates the verifying the peer connexion process with the subsequent creation of an incoming packet acceptance rule on a dedicated virtual interface – this allowed, due to multiple rules, to create a unique packet routing topology both in a dedicated network and in peer-to-peer (p2p) connexion between control controllers. An alternative conditional expression is a rule for redirecting packets through a virtual interface, due to which all traffic is processed through a secure connexion [12].

The process organisation of providing an devices IP pool can be provided through a trained language model (Fig. 3). It was previously noted that in the predicting a pool process of identical data sets, it is possible to use the NARX model, however, the text model advantages allow to obtain a more accurate set of identical output samples when solving reproducing identical results problems, as a result, the main model in this implementation is a text model based on a decoder [13].

Comparing similar existing text models, it is necessary to pay attention to the models “mpt-7b-instruct”, “vicuna-7b”, “nous-gpt4-vicuna-13b” – Table 1 demonstrates the results of executing an identical request for generating IPv4 address in network *172.15.1.0/24*.

Table 1. Comparison of the speed of execution of a text generation request.

Model	Answer	Request execution time (s.)
mpt-7b-instruct	172.15.1.100	5,41
vicuna-7b	172.15.1.25	6,85
nous-gpt4-vicuna-13b	172.15.1.65	11,24

The following were used as the main parameters for testing models: *batch size* = 25, *max_length* = 1000, *top-p token* = 0.92, *top-k token* = 45. The results of the comparison of the query execution speed with the specified parameters were carried out on the M1, 16 GB RAM processor. It is also worth considering that most of the text models do not involve targeted training on IP address datasets, and therefore the request processing speed is significantly lower than the execution speed of the limited model.

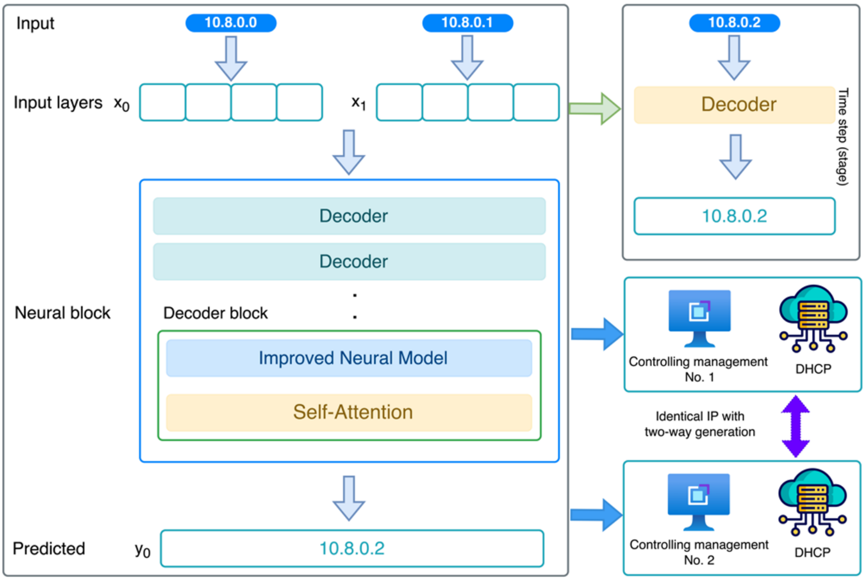


Fig. 3. IP pool prediction topology based on a text neural model

As can be seen from Fig. 3, the presenter model allow multi-step generation of a specific IP address for a given mask based on a trained model [14]. The main data processing process in the proposed model involves feeding data to the input vectors x_0, x_1, followed by autoregressive processing, involving the use of time t data at time *t+1*. In this case, the prediction of the token (ip address cell) *8* from the input address *10.8.0.0* is based on the token *10*.

It is worth noting that the implemented model also has API management, which allows to send and receive a request from a static model located on the same device. Among other things, the use of a trained model allows to set initial hardware requirements for further functional work, depending on the organisation scale, which will subsequently allow to provide the functionality of a decentralised VPN server for flexible work in organisations with a dynamic employees' location. At the moment, when implementing this solution, model 13B was used, designed for a *2048* characters sequence, with a steps number of *174335*, however, when solving this problem, the generation process is possible with 7B models.

2.2 Development of a dynamic DNS server for traffic redistribution

One of the most important controlling components is the step of processing and making decisions based on up-to-date data analytically produced during a given period. Most organisations that involve the multiple locations operation of the organisation's divisions do not assume the possibility of providing high-speed Internet or support for QoS billing systems, which has a direct impact on the decision-making process for the organisation's resources / making changes redistribution to the existing development strategy.

To solve this problem, it is proposed to develop a dynamic DNS server for load optimization when working via an external Internet network, while traffic encryption via DNSCrypt can be singled out as additional features [15]. The main stage in assigning a DNS server is to use the configuration of option *domain-name-servers* in *dhcpd* or *dhcp-option* DNS in OpenVPN server [16]. In this implementation, the problem of dynamic DNS server selection is proposed to be solved using a local server installed together with a VPN server, and with the appropriate assignment of the local interface address, as reflected in Listing 2. The DNS implementation main process involves the actual measurement of the current response from global servers like Google, Cloudflare, OpenDNS, Quad9, followed by the remote server replacement with the current one, while also providing the functionality of using a DNSCrypt proxy server as an additional ensuring the transmitted data security means (Fig. 4).

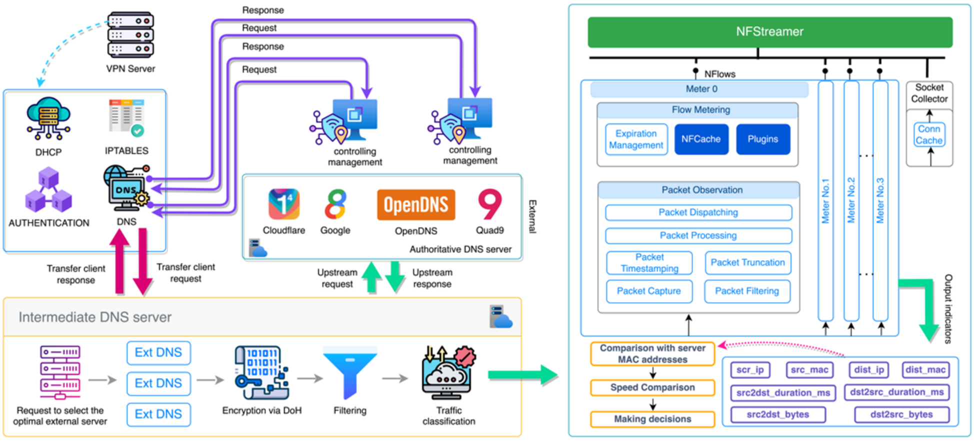


Fig. 4. Algorithm of DNS server interaction software modules

The representation of the specified algorithm for the DNS server interaction software modules uses a multi-module structure in its work, providing the possibility of flexible external DNS server selection based on the initial response from the request verification, followed by the provision of additional features – traffic encryption using DNS-over-HTTPS (DoH), filtering of certain content, as well as monitoring both by logging, and with the use of an additional traffic classification module. The main classification module uses the NFStreamer framework, which is based on the python language, and provides opportunities for monitoring packets within a network segment [17]. At the stage of its work, NFStreamer allows to monitor packets at the network card level with subsequent support for the output of multiple indicators – ip and mac addressing, response time from the source and destination addresses, as well as the bytes transmitted number in two-way mode. As a result, the use of this framework allows to monitor a specific port for a dedicated client (IP address) for use for organisational purposes, which in turn allows to monitor active operating system services for additional prevention of possible attacks.

The next step in the algorithm operation under consideration is the process of analytical changes comparison in the intermediate intervals of packet transmission between identical sets of addresses – in this case, if there is a coincidence in *scr* / *dist* addressing on the management decision-making server, a comparison of third-party client packets available for processing is performed in order to obtain consumable traffic per ms. The software implementation of this algorithm is performed using a module for predicting changes in the transmitted bytes of the client using a deep network based on the LSTM-XGBoost model [18-19].

The main advantage of using this model is the combining the correlation possibility of the dependence between the traffic amount and the transmission time – in this case, the initiated Q_i matrix is formed due to the vectors t_i, g_i, which represent data on the time interval (*ms*) and the amount of data (bytes) [20]. The activation function in this case is PReLU, which forms the output vector (Eq. 1).

$$\tilde{y}_{t+i} = PReLU(\varpi_i \cdot h_i + b_h), \tag{1}$$

At the stage of obtaining the output data and the LSTM model, the vectors prediction via XGBoost, represented by Eq. 2, is performed.

$$\tilde{y}_{t+i} = \sum\nolimits_{n=1}^{n} f_n(S_{t+q}), \tag{2}$$

where y_{t+i} is returning function the predicted values of XGBoost; S_{t+q} is output values of vectors from the neural network.

Thus, at this stage, preliminary data on possible traffic congestion is being obtained to adapt the operation of the control server. It is also important that the work chain of the DNS server allows to consistently process requests on internal and external servers.

2.3 Client authentication based on dynamic feature build-up

As the main methodology for client authentication based on multi-factor authentication, it is proposed to use early testing of primary client authentication methods based on methods correlation for obtaining a unique digital fingerprint with dynamic offset and subsequent authentication based on modification of the RSA algorithm. The method implementation is carried out identically to the mathematical function of obtaining a dynamic key according to Eq. 3, where the actions of the time interval are determined by the variable T.

$$\begin{gathered} target_{crypt} = MD5_{hash}((T_1 - T_0)\,/ \\ T \times normalise(identifier_{client}), \end{gathered} \tag{3}$$

were $target_{crypt}$ is dynamic authenticated sequence; T_1 is is current time value from the time package; T_0 is static time offset from the starting point in UTC; T is verification interval of the generated QR code; *normalise* is function of bringing the identifier to a normalised form; $identifier_{client}$ is the static server ID variable of the scientific and industrial cluster.

The two-way obtaining process of public and private RSA keys is based on the Euler function use as the input pattern of the training sample described by Eq. 4.

$$\begin{gathered} d \times e \equiv 1(mod\,\varphi(n)) \\ f = split(d(n), 13), \end{gathered} \tag{4}$$

were *f* is output value of the training sample pattern; *d* is multiplicative number; *d(n)* is generated full key; *split* is separation function.

At the next step, the predicted values of RSA keys are obtained, set by an identical trained model based on the previously specified text model. The practical implementation of this method was performed in python, and the main library for neural network processing was tensorflow [21].

The input point for forecasting is the offset *0x*, and as weights – a custom model of the h5 format. In this example, LSTM and DENSE layers are also used, with a dimension of 256 neurons and a *softmax* activation function, respectively. As a result, the output vector converted into a char sequence is the public RSA key of dynamic authentication.

Thus, in the proposed algorithm, secure access is carried out due to the initial installation of the organisation identifier, on the basis of which a unique sequence is generated, verification of which is carried out in a two-way mode using the decision-making module.

3 Results and discussion

As the main result of managing the implemented information flow distribution system, can single out the software module of the decision support system (DSS) for convenience, coordination and visibility of the practical operation of the VPN protocol in the organisations interaction. Taking into account the fact that several decision-making points can be identified in the developed interaction management system, such as DHCP synchronisation of clients, traffic redistribution, client authentication, it is advisable to use a distributed decision-making system based on fuzzy logic [22]. The existing decision-making tools mostly involve working in linear mode with conditional expressions, but it is possible to use fuzzy logical methods based on multiple variations of the predicted values described earlier, which allows to optimally quickly and accurately extract the percentage of matches across two data arrays. These functions were implemented through the configuration of several logic modules (Fig. 5).

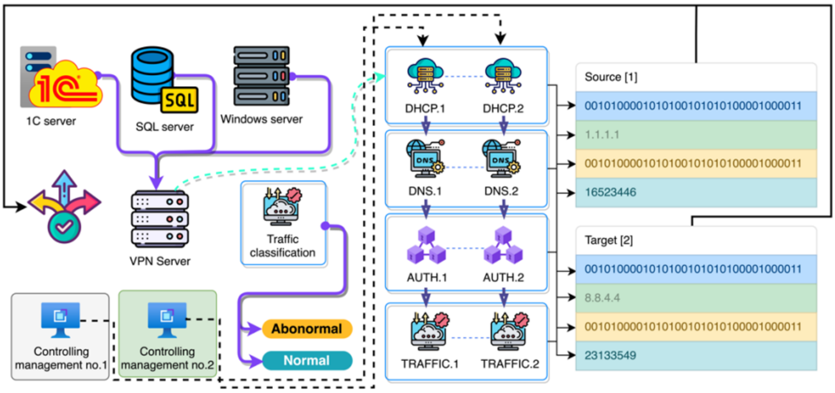
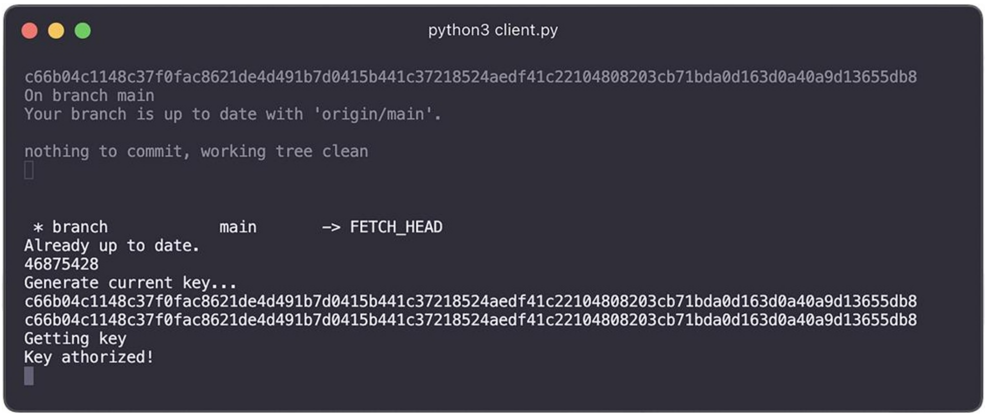


Fig. 5. Process of comparison and decision-making in a multimodule system

As can see from the Fig. 5, the software implementation of the decision-making module is based on the FuzzyWuzzy library, where the character-by-character comparison process of authentication blocks each, address assignment, DNS, as well as possible discrepancies in traffic is applied. The described proposed system result, taking into account the receipt of various variations of responses to each of the DHCP, DNS, AUTH, TRAFFIC modules, will form an objective basis for decision-making by controlling specialists in organisations on changes in the operation of the virtual network. The Python programming language was chosen as the main means of conducting experimental testing of the implemented client authentication algorithm (Fig. 6).

The secondary window, in turn, is a client that generates a sequence and compares it with the original one on a remote server after an identical time interval. As can be seen from the test result, the requests for comparing two keys are successful, which indicates the successful development of a client authentication algorithm.



```
c66b04c1148c37f0fac8621de4d491b7d0415b441c37218524aedf41c22104808203cb71bda0d163d0a40a9d13655db8
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean



 * branch            main       -> FETCH_HEAD
Already up to date.
46875428
Generate current key...
c66b04c1148c37f0fac8621de4d491b7d0415b441c37218524aedf41c22104808203cb71bda0d163d0a40a9d13655db8
c66b04c1148c37f0fac8621de4d491b7d0415b441c37218524aedf41c22104808203cb71bda0d163d0a40a9d13655db8
Getting key
Key athorized!
```

Fig. 6. Testing the client authentication algorithm based on dynamic encrypted data

As a result, can say that the development of the proposed solution, along with the fuzzy comparison function, will also allow for successful authentication in the presence of possible discrepancies in the event of interference in the software component of the client-server equipment.

4 Conclusion

The study of decision support systems for controlling specialists implementing the automated information flow management functions using applied software solutions has revealed a number of urgent problems. Among them, can highlight the lack of open software development with security support and optimised work in organisations with a decentralised network. As a solution to this problem, the development of an intelligently distributed system for controlling information flows was carried out, based on the virtual VPN server formation with the work adaptation in various TCP/IP topologies. The main advantage of this development is a two-way DHCP server that performs parallel controller’s synchronisation in p2p mode using a trained text model. The development of a dynamic DNS server made it possible to adaptively select an up-to-date external query processing server, and the combination of the NFStreamer framework made it possible to receive up-to-date information about transmitted packets for the traffic optimization operation module based on the LSTM-XGBoost model. The decision-making process, along with the subject authentication module, also made it possible to automate the multifactor verification process of data both at the ensuring security stages and optimising the virtual network operation. Among the limitations of the presented system, one can single out the need for the primary assignment of the key of interacting subjects, as well as the need to retrain the neural network model taking into account changing parameters for a particular organisation. The results of the study also made it possible to make a significant contribution to the theory of deep learning, decision support systems, systems for building adaptive decentralised TCP/IP topologies development. Especially particular note is the experimental testing process of client-server authentication, which can later be used as a method of two-way data verification, which also makes a significant contribution to the field of improve data security.

Thus, the proposed intelligently distributed system of controlling information flows allows not only to reduce the time spent on collecting, processing and analysing data between individual entities responsible for presenting information and making informed management decisions, but also significantly improve the safety of such work. The described solution security and reliability will facilitate the translation of an increasing amount of information about the organisations business processes into a digital format, in which they will be processed and presented to the decision-maker in a clear and understandable form.

5 Acknowledgements

The research was supported by RSF (project No. 22-21-00487).

References

1. E. A. Kasyuk, *Development of conceptual approaches to understanding the essence of the category 'Controlling'*, Herald of Siberian Institute of Business and Information Technologies, **11**, 106-110 (2022) doi:10.24412/2225-8264-2022-4-106-110
2. L. Reny, Y. Ren, Oracle Hyperion FDMEE Basics: A Step-by-Step Study Guide for FDMEE Entry-Level Professionals (Hyperion Step by Step), Independently published (2020)
3. O. L. Golubeva, *Analysis of the modern ERP systems functionality*, Management in modern system, **3(35)**, 43-58 (2022) doi:10.24412/2311-1313-35-43-5
4. F. Franzen, L. Steger, J. Zirngibl, P. Sattler, *Looking for Honey Once Again: Detecting RDP and SMB Honeypots on the Internet*, in Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops, EuroS&PW, 06-10 June 2022, Genoa, Italy (2022) doi:10.1109/EuroSPW55150.2022.00033
5. Y. Kraev, G. Firsov, D. Kandakov, *Authentication via RDP Using Electronic Identifiers*, in Proceedings of the 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus, 26-29 January 2021, St. Petersburg, Moscow, Russia (2021) doi:10.1109/ElConRus51938.2021.9396471
6. A. Jain, S. Bhullar, *Network performance evaluation of smart distribution systems using smart meters with TCP/IP communication protocol*, Energy Reports, **8**, 19-34, (2022) doi:10.1016/j.egyr.2022.05.108
7. N. B. Daimen, V. a-p Selvarajah, *Jamming Windows OS Through DDoS*, in Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference, MysuruCon, 16-17 October 2022, Mysuru, India (2022) doi: 10.1109/MysuruCon55714.2022.9972619

8. J. Carrillo-Mondéjar, J. L. Martinez, G. Suarez-Tangil, *On how VoIP attacks foster the malicious call ecosystem*, Computers & Security, **119**, 102758 (2022) doi: 10.1016/j.cose.2022.102758
9. K. G. Mehrotra, C. K. Mohan, H. Huang, Anomaly Detection Principles and Algorithms (Terrorism, Security, and Computation), Springer (2018)
10. M. S. Tok, M. Demirci, *Security Analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard*, Computers & Security, **109**, 102394 doi: 10.1016/j.cose.2021.102394 (2021)
11. E. R. Estaño, L. E. Wiesse, C. A. Goyzueta, *IPv6 Plug and play business firewall design based on Iptables, Nettop and linux*, in Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering, ICECCME, 07-08 October 2021, Mauritius, Mauritius (2021) doi: 10.1109/ICECCME52200.2021.9591064
12. P. L. S. Kumari, C. H. S. devi, S. Thivaharan, K. Srinivas, A. Damodaram, *A resilient group session key authentication methodology for secured peer to peer networks using Zero knowledge protocol*, Optik, **273**, 170345 (2023) doi:10.1016/j.ijleo.2022.170345
13. A. Zaenchkovski, A. Lazarev, D. Tukaev, V. Epifanov, *Intelligent Information Flow Management System in innovative scientific and industrial clusters*, IJPEDS, **37**, 303-317 (2022) doi: 10.1080/17445760.2022.2060976
14. L. Xuyuan, T. Lihua, L. Chen, *TCTG:a controllable text generation method using text to control text generation*, in Proceedings of the 2021 IEEE 6th International Conference on Signal and Image Processing, ICSIP, 22-24 October 2021, Nanjing, China, (2022) doi:10.1109/ICSIP52628.2021.9688767
15. O. Arana, H. Benítez-Pérez, J. Gomez, M. Lopez-Guerrero, *Never Query Alone: A distributed strategy to protect Internet users from DNS fingerprinting attacks*, Computer Networks, 199, 108445 (2021) doi:10.1016/j.comnet.2021.108445
16. J. Keijser. OpenVPN Cookbook. 2nd edition, Packt (2017)
17. Z. Aouini, A. Pekar, *NFStream*, Computer Networks, **204**, 108719 (2022) DOI: 10.1016/j.comnet.2021.108719
18. M. I. Dli, Y. V. Sinyavsky, E. I. Rysina, M. A. Vasilkova, *A method for classifying mixing devices using deep neural networks with an expanded receptive field*, Journal of Applied Informatics, **17**, 51-61 (2022) doi:10.37791/2687-0649-2022-17-5-51-61
19. B. Ren, L. Chen, H. Ma, X. Xue, *A robust short-term wind power forecasting algorithm based on LSTM-XGBoost model*, in Proceedings of the 2021 IEEE 5th Conference on Energy Internet and Energy System Integration, El2, 22-24 October 2021, Taiyuan, China (2022) doi:10.1109/EI252483.2021.9713102
20. I. Palari, A. Karanikola, S. Kotsiantis. *A comparison of the optimized LSTM, XGBOOST and Arima in time series forecasting*, in Proceedings of the 2021 12th International Conference on Information, Intelligence, Systems & Applications, IISA, 12-14 July 2021, Chania Crete, Greece (2021) doi:10.1109/IISA52424.2021.9555520
21. D. Akgun, *Tensorflow based deep learning layer for local derivative patterns*, Software Impacts, **14**, 100452 (2022) doi: 10.1016/j.simpa.2022.100452
22. D. Pekaslan, C. Wagner, J. M. Garibaldi, *Adonis—Adaptive Online nonsingleton fuzzy logic systems*, IEEE Transactions on Fuzzy Systems, **28**, 2302-2312 (2020) doi: 10.1109/TFUZZ.2019.2933787