ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

Development of a network attack detection approach on distributed information systems

Rakhmanova Gulnora Sadirovna,Khaydarbekova Mokhira Mirrashidovna

Senior Lecturer, Power Supply Systems Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
Senior Lecturer, Power Supply Systems Department, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

ABSTRACT. In this article an approach for combining batch processing on master and slave nodes in order to effectively communicate the dynamics of processing big data is developed. The schemes of methods of data collection in static and dynamic mode are proposed.

I. INTRODUCTION

DoS or denial of service attack is aimed at the computing system in order to create conditions under which users of the system cannot get data to certain resources or services. A simultaneous attack from a large number of computers indicates DDoS attack - a distributed denial of service attack. Such attacks are used when it is necessary to cause a denial of service to a well-protected company or government organization. Such attacks are carried out using computers infected with special trojans, which are often called “zombie computers”.

II. PARTICLE SWARM METHOD

When developing a methodology for detecting network attacks, the particle Swarm method (PSM) is considered as a solution. It becomes necessary to create a systematized class of solvers for collecting software Big Data. In the data collection approach, two functions are added and implemented:
1. Initialize (partArray: Particle [..,.], _ Size: const int) - initial setup of the selector, binding strategies, parameters, and functionality to particles.
2. Update (...) - update the internal state of the selector, adaptation to external conditions. By default, it is executed at each iteration. Summing up, it is important to note that a task of the Iterative Method type is solved by the following formula:

$$W = \frac{V \times X}{t} \qquad (1)$$

Where $W -$ invariably efficiency coefficient of the typed solutions PSM; V, $X -$ vectors of particle velocity and coordinates; $t -$ iteration number.
The diagram connecting the components can be represented by the circuit depicted in Fig.1.

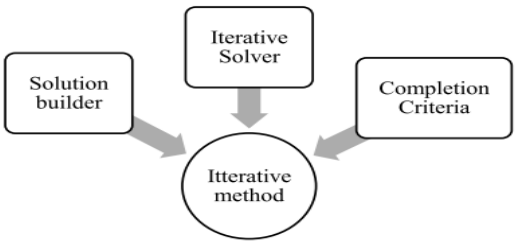

Fig.1. Diagram of some abstract solver for data collection

An important factor in the data collection technique is the elimination of possible errors in this mechanism[1]. Having data on the analysis of error occurrence frequencies, it is necessary to derive a statistical analysis of the operation of Big Data on PSM, which shows a comparative assessment of the results of random errors in data transmission, which is possible by the formula:

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

$$F = \sum_{n=0}^{=} \frac{S_n}{n!} W \qquad (2)$$

where F −evaluation of the results of random errors in data transmission;W − is the coefficient of effectiveness of the decisions made according to the PSM.

Having (2) it is possible to find out on what types of operator replacements the risk of an accidental error in data transmission decreases or increases. Bearing in mind the need for subsequent application of data collection methods, it is important to have a procedure for implementing reliable collection and storage of information.

The approach distinguishes between static and dynamic modes of operation of the entire network attack detection system.

III. THE SCHEME OF THE METHOD OF COLLECTING DATA IN STATIC MODE

The output obtained at each stage is used as input to the next stage. Data movement between steps is shown by arrows (Fig.2).

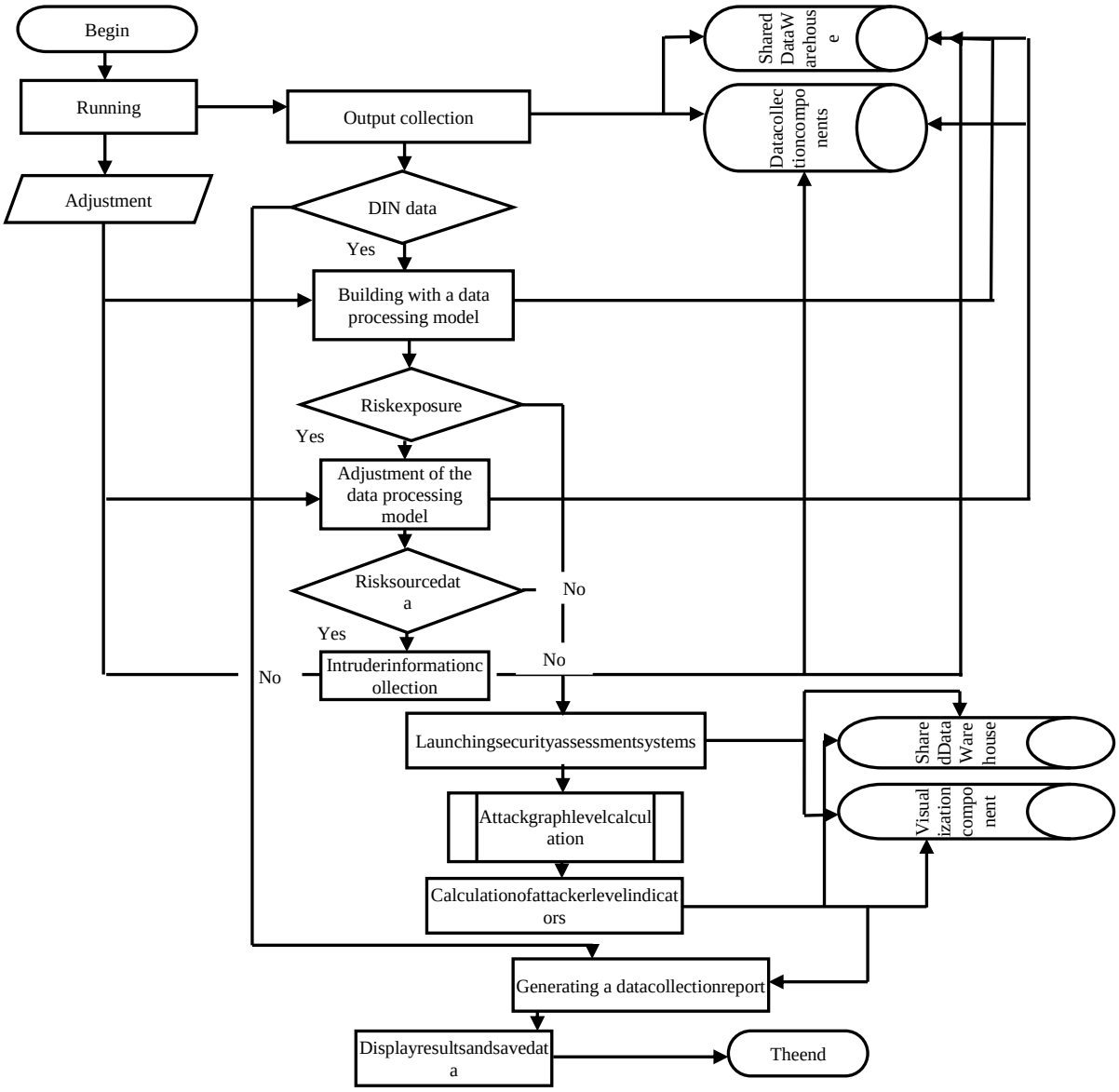

Fig. 2. The block-scheme of the method of collecting data in static mode (first step)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

In more detail, the stages of the method in dynamic mode and the sequence of their implementation are presented in Fig. 3.

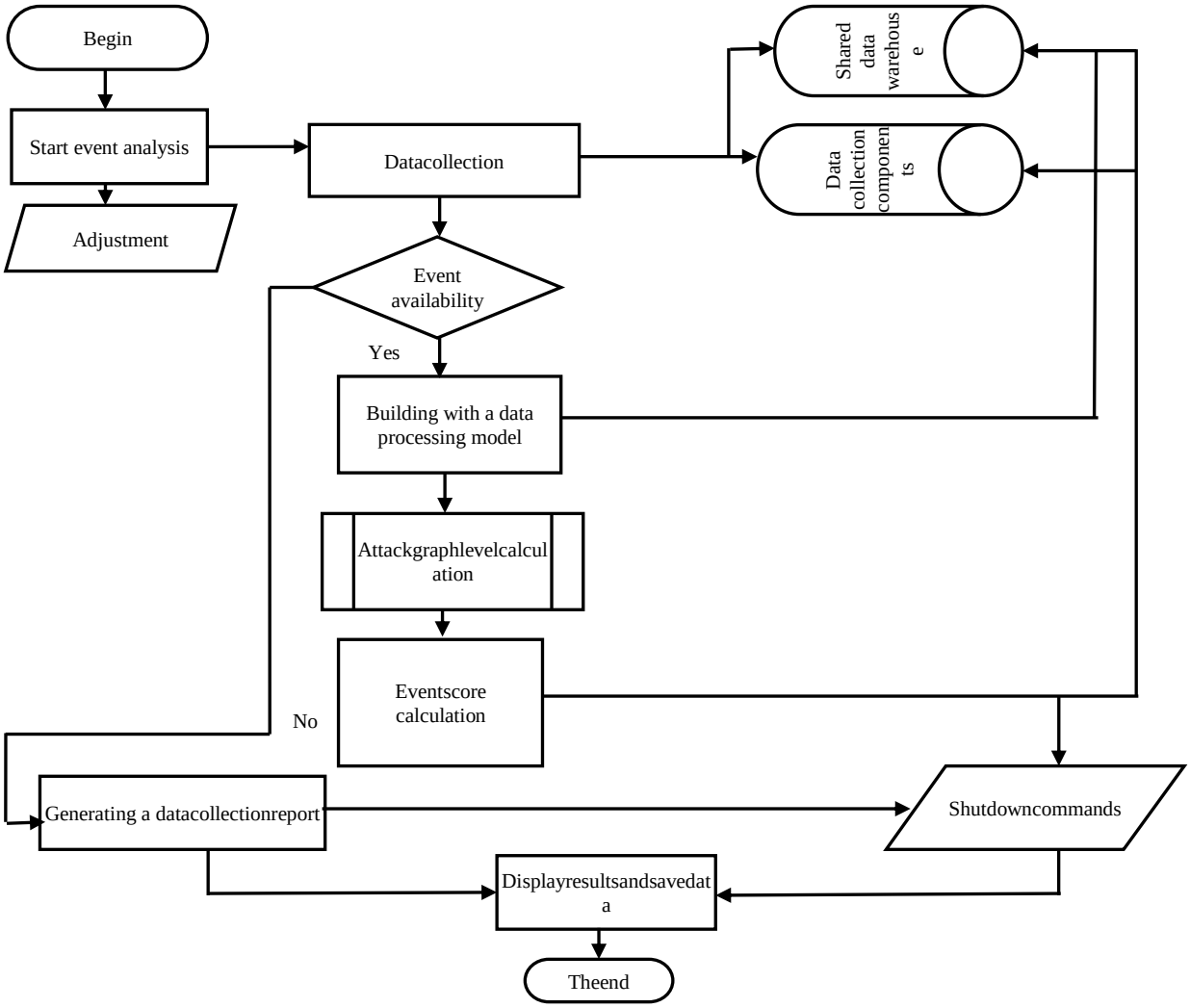

Fig. 3. The block-scheme of the method of collecting data in dynamic mode(first step)

The indicated threshold value of the increase in information collection $k_{collection}$ (data collection coefficient without error) allows you to set the required value for the used values of N_{bit} (the amount of processed information in bits), which will then be guided by the value of S_n. The S_n value is determined as the dependence of the Big Data characteristic, on the example of which the successful amount collected in distributed information networks (DIN) is known in advance.

Since the parameters are related to the general interaction with bit exchanges in executable files, any change in F may depend on these parameters, because there is a value of S_n.

$$k_{collection} = e^n S_n \quad (3)$$

where

$e^n -$ exponential function to verify the effectiveness of all data collection techniques.

Formula (3) will be responsible for predicting the successful processing of information for users in the DIN, where there are potential errors and intrusion threats [2-3]. This means that the coefficient $k_{collection}$ will affect the degree of security in the data processing model.

If the first stage was to determine the risks and errors for data collection, the second stage is to parallelize the tasks during their final processing while reducing the time to detect intrusions. The implementation of the claimed second stage is illustrated by the algorithm (Fig.4), which works on the central node in the data flow processing model. Using

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

and combining the techniques described above allows you to make serious protection [4-5]. This technique is supplemented by the following: the concepts of collection fields are introduced to the "upgrade" of data collection, namely "Big Data Lifetime" (T), "Big Data Options" (O), "Destination Addresses" (D), "Source Addresses" (I), which are stored in arrays formed for them.

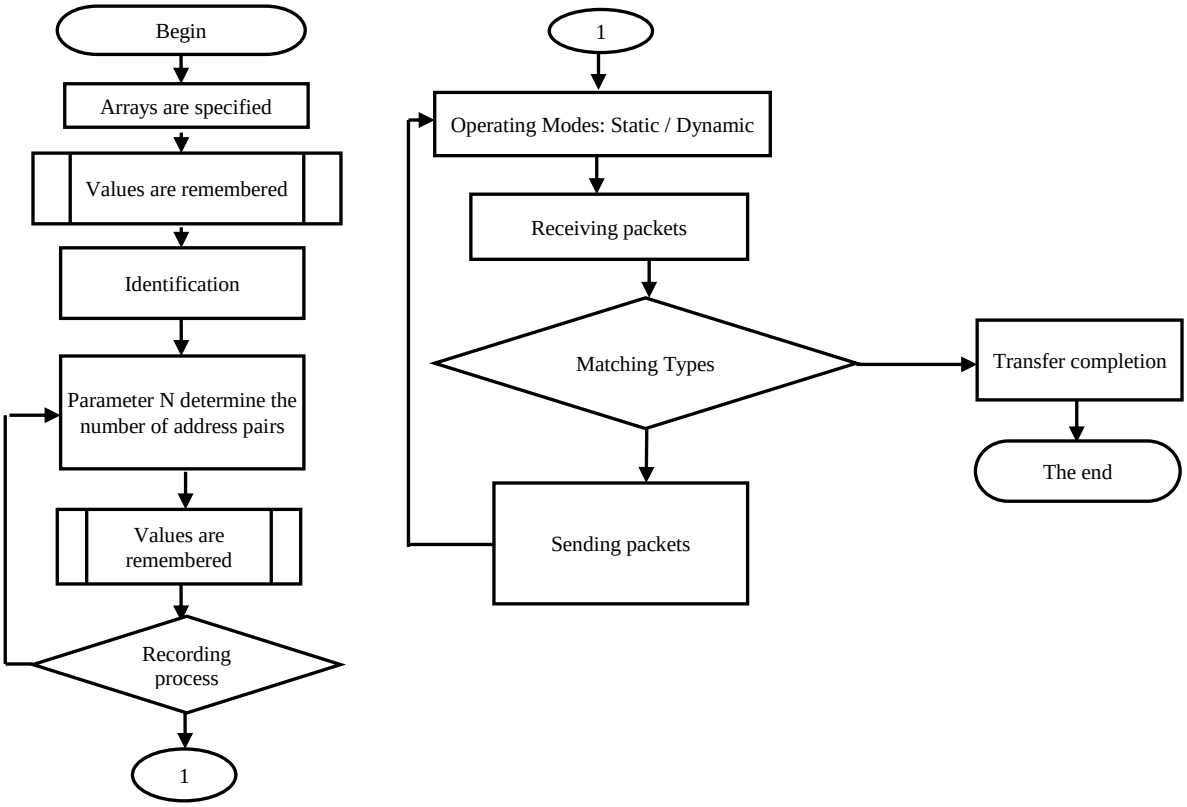

Fig.4. Data collection at a central site(second step)

Based on this, for the network attack detection system, a planned monitoring is built during data collection (Fig. 5) to maintain operability.

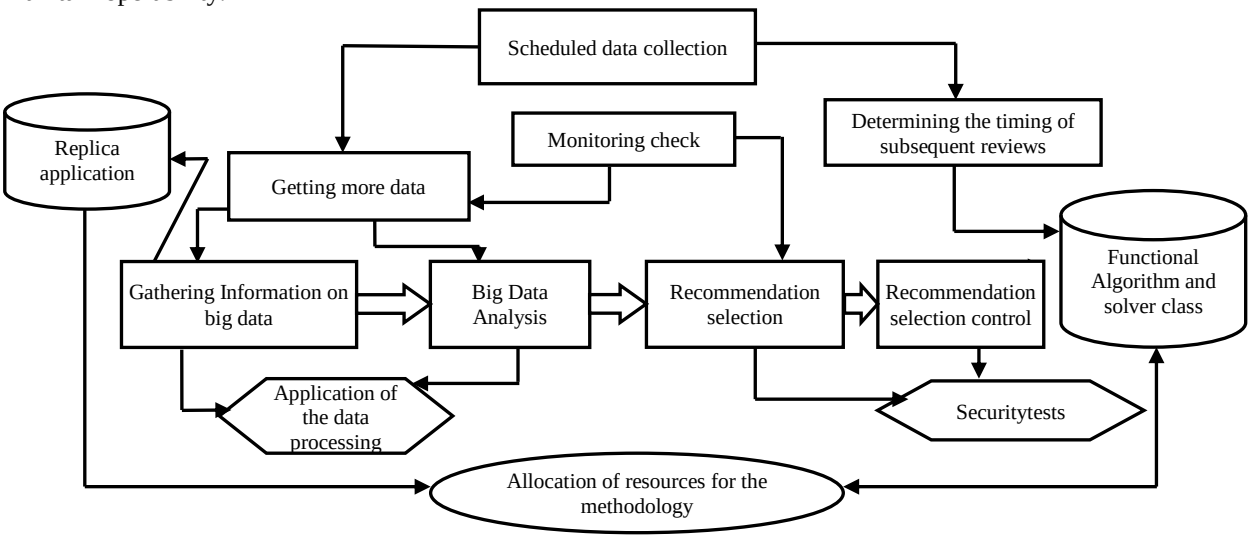

Fig.5. Data collection monitoring(second step)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 6, Issue 12 , December 2019

For the proposed methodology, the following rule was identified that, with a general percentage, the collection is carried out according to the criteria of the software used in them [6]. The two-stage approach of the technique is laid in a special equation that selects the necessary parameters. The equation consists of the following parts:

1. Determination of probability density. If the probability P is absolutely continuous, then according to the Radon-Nikodemus theorem, there exists a non-negative Borel function $f: p^n \to [0, \infty)$ such that:

$$p^n = \int f(x)dx \quad (4)$$

2. Normal probability distribution (Gaussian-Laplace distribution). According to it, for the second approach, methods are taken, each of which makes a small contribution with respect to the total amount for data collection, then with an increase in the number of terms the distribution of the centered and normalized result tends to normal. For the second approach, the following statement is true:

$$f(x) = \frac{1}{\sigma\sqrt{2dx}} P^{-\frac{(x-\mu)^2}{2\sigma^2}} \quad (5)$$

where $\mu -$ is the mathematical expectation (average value), and the parameter $\sigma -$ is the standard deviation of the distribution.

Based on this, at the second stage, a mechanism is formed for the agent, which will control all incoming flows.

IV. AGENT POLYMORPHIC ALGORITHM GENERATOR

Consider the construction of a generator of polymorphic algorithms for an agent (Fig.6).

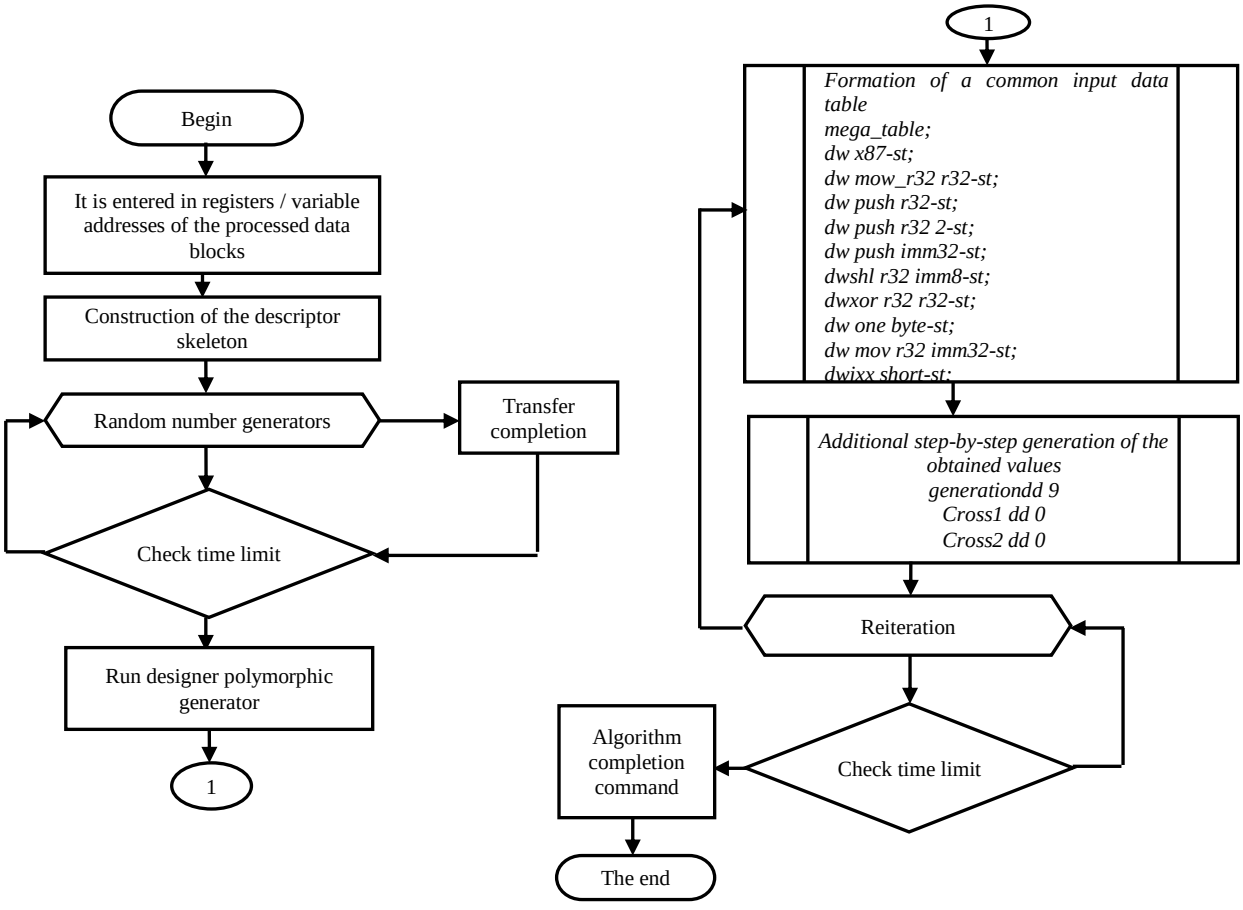

Fig.6.Typical block-scheme of the running of individual mechanisms of a polymorphic agent generator(second step)

This block diagram is always generated in pairs, the mechanism of their generation is very similar and is carried out by

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

the same code with encryption / decryption algorithms.In Table 1 below, based on the results of functional work in synchronizing the processing model and the network attack detection technique, it became possible to present a comparison of the proposed results [7]. This table shows which additions are also possible while simultaneously operating in static and dynamic modes at both stages (phases) of data collection.

Table 1. Comparison of models and techniques for detecting network attacks

Features	Data processing model	Data collection methodology
Cluster sizes for processing	Large cluster	Small cluster
Data set	Multiple Related Datasets	One dataset
Cluster locations	Tables and data are permanently in the cluster	
Table resizing	The size of the tables (and the intensity of queries to them) remains stable over time	
Measurement Types for Approaches	There is a dimension in the data by which it can be segmented, and there are almost no queries that affect data located in several segments	The data has homogeneous and heterogeneous queries
Storage method	Decentralized	Centralized
Opportunities	Identify hidden dependencies and search for new questions and answers based on the analysis of the entire volume of heterogeneous data	Data analysis not only from internal, but also from external sources

In synchronizing results, it is possible to execute queries faster than in campaigns from the SQL-on-Hadoop class family. This is because in the data processing model:

1. Perhaps you need your own format for monitoring users, as they are closely integrated with query processing engines.
2. Data is distributed relatively “statically” between nodes, and this can be used for distributed query execution. It is assumed that the accuracy of detecting anomalies in the processing and collection of Big data, and the advantage in the case of a two-stage approach depends on the number of parameters taken into account and the quality of analysis.

V. CONCLUSION

In conclusion, it should be noted that for the network attack detection system, planned monitoring is being built during data collection in order to maintain operability, and it is assumed that the accuracy of network attack detection during Big Data processing and collection, and the advantage in the case of a two-stage approach depends on the number of parameters taken into account and quality analysis..

REFERENCES

[1] Deshevix E.A. Integration of SIEM systems with correlation systems of security events based on big data technology // Information Technologies in Management (ITU-2016) Materials 9th conference on management issues. Chairman of the Presidium of the multiconference V. G. Peshekhonov. - 2016.- S. 684-687.

[2] Brindasri, S. Evaluation of Network Intrusion Detection Using Markov Chain / S. Brindasri, K. Saravanan // International Journal on Cybernetics &Informatics (IJCI). — 2014. — Vol. 3, no. 2. — Pp. 11–20.

[3] Day, D. A performance analysis of snort and suricata network intrusion detection and prevention engines / D. Day, B. Burns // In Proceedings of theFifth International Conference on Digital Society (ICDC), Gosier, Guadeloupe. — 2011. — Pp. 187–192.

[4] Ennert, M. Testing of IDS model using several intrusion detection tools /M. Ennert, E. Chovancova, Z. Dudlakova // Journal of Applied Mathematicsand Computational Mechanics. — 2015. — Vol. 14, no. 1. — Pp. 55–62.

[5] Komar, M. Development of neural network immune detectors for computer attacks recognition and classification / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov // In Proceedings of the 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). Vol. 2. — IEEE. 2013. — Pp. 665–668.

[6] GulomovSh.R., Ganiev A.A. Methods and models of protecting computer networks from un-wanted network traffic. International Journal of Engineering & Technology, Indexed in Scopus. Vol 7 No 4 (2018)Science Publishing Corporation, RAK Free Trade Zone, RAK FTZ Business Park, Business Centre 4,Al Mamourah Area, P.O. Box: 487447, UAE, – P.2541-2545

[7] Mehra, P. A brief study and comparison of snort and bro open source network intrusion detection systems / P. Mehra //International Journal of Advanced Research in Computer and Communication Engineering. —2012. — Vol. 1, no. 6. — Pp. 383–386.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 6, Issue 12 , December 2019

AUTHOR'S BIOGRAPHY

RakhmonovaGulnoraSadirovnawas born September 19, 1963 year in Tashkent city, Republic of Uzbekistan. In 1985 graduated «Engineer economics» faculty of Tashkent Polytechnic Institute. Has more than 65 published scientificworks in the form of articles, journals, theses and tutorials. Currently works at the department «Power Supply Systems» in Tashkent University of Information Technologiesnamed after Muhammad al-Khwarizmi.

KhaydarbekovaMokhiraMirrashidovnawas born 1964 year in Tashkent city, Republic of Uzbekistan. In 1986 graduated «Automatic communications engineer » faculty of Tashkent University of Information Technologies. Has more than 60 published scientificworks in the form of articles, journals, theses and tutorials. Currently works at the department «Power Supply Systems» in Tashkent University of Information Technologiesnamed after Muhammadal-Khwarizmi.