Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/22343
DOI URL: http://dx.doi.org/10.21474/IJAR01/22343

RESEARCH ARTICLE

USING GENETIC ALGORITHMS TO OPTIMISE CYBERSECURITY PROTOCOLS IN DATA MANAGEMENT SYSTEMS

Oboulhas Tsahat Conrad Onesime and Nkouka Moukengue Charmolavy Goslavy Lionel

1. Ecole Nationale Supérieure Polytechnique,Universite Marien NGOUABI, Republic of Congo.

Manuscript Info

Manuscript History
Received: 4 October 2025
Final Accepted: 6 November 2025
Published: December 2025

Key words:-
Data management, cybersecurity, genetic algorithm, analytics, protocol.

Abstract

Faced with the increasing complexity of cyberattack scenarios against information systems, ensuring the proper functioning of multi-layered protection systems requires the synchronization of all components, both at the overall system level and at the level of its individual components at each line of defense.Intelligent data analysis methods and approaches make it possible to solve these problems efficiently and at a lower cost. This article aims to study the practical aspects of using a genetic algorithm to optimize cybersecurity protocols in data management systems. It presents an approach for selecting the optimal set of cybersecurity protocols based on a genetic algorithm and data analysis. One of the major strengths of this approach lies in its ability to simultaneously optimize different cybersecurity protocols based on specific target functions. Test results on the algorithm demonstrate that it is a practical tool for developing an information protection strategy that is both effective and cost-effective. A distinctive feature and advantage of this approach is the ability to simultaneously optimize various cybersecurity protocols in accordance with specified target functions. The results of testing the algorithm indicate that it provides a practical tool for forming the most effective and economically feasible information protection strategy.

Introduction:-

Automated design methods are of great importance in the process of creating and deploying information security systems for computer complexes and databases of various informatization objects. These methods are particularly important in the process of developing and agreeing on cybersecurity protocols for critical digital platforms that handle sensitive data, such as medical information about patients, financial transactions, proprietary industrial information, etc. [1]. The confidentiality, integrity, and availability of this data are of paramount importance, as any breach could have serious consequences, such as economic losses, reputational damage, and potentially life-threatening situations.Successful data management strategies must ensure that information has not been tampered with at any point during its lifecycle, does not contain malicious, unwanted, or unauthorised content, and does not have unintended duplicates or anomalous information [2].Current practice shows that security issues in data management systems are addressed using firewalls, antivirus software, intrusion detection systems (IDS), integrity

Corresponding Author:- Oboulhas Tsahat Conrad Onesime
Address:-Ecole Nationale Superieure Polytechnique, Université Marien NGOUABI, Republic of Congo.

control systems, cryptographic protection tools, etc. [3]. These methods are typically used either periodically and briefly to solve a specific problem, or continuously but with static settings. At the same time, the growing complexity of successful cyberattack scenarios targeting various information systems, including complex information security systems, as well as the dynamic changes in the cyber threat landscape, mean that the task of constantly improving security protocols is becoming increasingly important, as existing systems are unable to provide a high level of protection. The relevance of this task is clearly demonstrated by the data presented in Table 1

Table 1 Security protocols and mechanisms most vulnerable in data management systems

Application sector	Average losses per incident	Key gaps and vulnerabilities	Protocols and technologies that are sources of problems
General corporate networks	4.5 million dollars per incident	Lack of end-to-end encryption, outdated algorithms	SSL 3.0, TLS 1.0–1.1, use of RC4, MD5, weak IPSec implementation
Financial sector	6.0 million dollars	Key compromise and vulnerabilities in API interactions	OAuth 1.0a, unprotected REST APIs without signatures, JWT without encryption, leaks in HTTPS downgrade
Healthcare	10.9 million dollars	Personal data leaks due to the use of unsecured transmission channels between local servers and cloud services	FTP/SFTP without key authentication, SMTP without TLS, older versions of HL7 v2.x without encryption
Industry and IoT	3.8 million dollars	Unauthorised access to controllers and sensors, interception of telemetry data	Modbus/TCP, DNP3, OPC-DA — open data transmission without cryptographic protection
Government and energy systems	5.1 million dollars	Lack of centralised authentication and access logs	RADIUS without EAP-TLS, SNMP v1/v2, Telnet, open SSH channels without key pairs
Corporate MDM systems	3.2 million dollars	Leaks due to weak authorisation policies and unprotected exchange between nodes	LDAP without TLS, Kerberos with static keys, unprotected HTTP/JSON API connections
Cloud and distributed data storage systems	4.7 million dollars	Access violations, API key leaks, incorrect encryption configuration	AWS IAM without MFA, SMBv1, NFS without Kerberos, outdated SSH keys and SSL certificates

Solving the problem of building multi-contour protection systems in conditions of increasing attempts to destructively impact databases and their management systems requires the use of not only classic optimization procedures, but also more universal methods, such as genetic algorithms (GA), which have proven their effectiveness in various fields.
The importance of applying GAs in cybersecurity issues cannot be overestimated. First and foremost, they can solve problems for which there is no exact analytical solution or which are large and complex [4]. Due to the nature of stochastic search, GAs are capable of finding acceptable solutions even in spaces with many local maxima or minima. Another important aspect is the ability of GAs to work with nonlinear and non-differentiable functions. This is especially useful in tasks of providing comprehensive protection of big data, where a significant number of criteria and parameters interact with each other [5].Thus, the current scientific and technical challenge is to develop effective, comprehensive methods for protecting data management systems using GAs and data analytics, with an emphasis on the development and application of advanced and effective protocols capable of providing a modern level of protection and authentication, which determined the choice of the topic of this article.

Literature Review:-

It should be noted that the ever-relevant task of forming effective cybersecurity contours in data management systems has prompted numerous studies devoted to optimizing the composition of information protection measures. These studies are primarily aimed at answering questions related to solving multi-criteria optimization problems, which are characterized by such features as: the complex configuration of the permissible scope of application of individual information protection protocols; the multi-extremality of the functions under consideration; the algorithmic task of functions, etc.Zhai J., Li Z., Miao H., Li Z., Zhou X., Yang H. [6], Ahmad, J., Zia, M. U., Naqvi, I. H., Chattha, J. N., Butt, F. A., Huang, T., Xiang, W. [7], Vasinev D.A. and Solovyov M.V. [8], Klishin and Chechulin [9]. The authors consider criteria such as the time to detect and respond to threats, which reflects the effectiveness of monitoring systems and incident response plans. Another important indicator—the number of vulnerabilities identified and

eliminated—shows the effectiveness of risk assessment. In addition, the researchers argue that the level of employee compliance with training and protocol requirements can also reveal gaps in their awareness. Separate emphasis is placed on the fact that tracking uptime and system downtime caused by cyber incidents provides insight into operational resilience.However, despite the wide range of indicators and criteria, a unified and consistent, adaptable and expandable methodology for assessing cyber resilience has not yet been developed. In addition, publications do not specify what measures need to be taken to ensure that the assessment of protocol effectiveness is repeatable and reproducible and that the indicator can be interpreted correctly.

In the work of Lone AN, Mustajab S, Alam M. [10], Zeng, L., An, Y., Zhou, H., Luo, Q., Lin, Y., Zhang, Z. [11], Kirillova A.D. et al.[12], and Sarker I.H. [13] propose feature selection models for network intrusion detection systems based on PSO, GWO, FFA, and GA algorithms. To evaluate the selected features from the UNSW-NB15 dataset, the authors used SVM and J48 classifiers and analysed the effectiveness using the metrics of accuracy, precision, sensitivity, f-measure, TNR, FPR, FNR, and TPR. The best results were obtained using the J48 algorithm, where accuracy was 90.48%, precision was 84.13%, sensitivity was 97.14%, f-measure was 90.17%, and FPR was 2.859%. At the same time, the works lack analysis of important features selected by algorithms, do not take into account the time required for model training, and do not compare the obtained experimental results with other studies. The authors Alsadie, Deafallah [14], Fatin A.D. [15], Heydari M., Shabgahi G. I. and Mohammad Mehdi Heydari [16], Sarah Vluymans [17] describe in detail the main functions of ensuring the information security of data management systems. In addition, two approaches to detailing and formalizing the distribution of resources between different information protection functions were proposed. The first approach is based on the need to consider the composition and quantity of these resources. The second involves analyzing generalized patterns and relationships between different protection methods and the effectiveness of their application. However, despite a well-reasoned approach and detailed description, the works do not provide specific examples of the application of the proposed optimization models.

Scientists from around the world are working on the development of the concept of security for socio-cyber-physical systems and the integration of cyber threats into information protection components and protocols. For example, Ding, S., Lu, S., Xu, Y., Korkali, M., Cao, Y. [18] analysed issues of interaction between technological platforms and centres aimed at ensuring the stability and integrity of data in smart city subsystems. Green, M., Sarkani, S., Mazzuchi, T. [19] studied the specifics of the formation and practical application of the concept of comprehensive information protection in modern distributed systems. While highly appreciating the results obtained, it should be noted that most studies are theoretical in nature and do not consider the practical aspects of implementing intelligent analysis technologies in the cybersecurity contours of modern information systems.Thus, considering the above, the purpose of this article is to study the practical aspects of using GA to optimize cybersecurity protocols in data management systems.

Research Methodology:-

Research methodology is based on a comprehensive scientific and technical approach, including an analytical review of current publications and industry reports on the optimization of cybersecurity protocols in data management systems, as well as the application of mathematical modelling and computational experiment methods. The study used tools of system and structural analysis, formalization and modelling to describe the functioning of protection measures and evaluate the effectiveness of protocols. The practical part was carried out in the form of simulation modelling and testing of the developed algorithm on model data, which made it possible to quantitatively evaluate the optimization results and confirm the applicability of the proposed approach for complex data management systems.

Results and Discussion:-

The use of GA and intelligent data analysis tools significantly expands the possibilities for improving cybersecurity protocols by improving threat identification and response processes. This approach is based on typical applications of GA in function selection and optimization, as well as on advanced evolutionary search methodology to improve the reliability of protection systems [20].The solution proposed in the article is based on a general evolutionary algorithm and its multi-criteria GA components. The main method used is VEGA - Vector Evaluated Genetic Algorithm [21,22]. This method provides for the extension of the traditional GA, which is implemented by applying vector estimates of the fitness of instances (individuals), as well as the ability to simultaneously evaluate populations for each criterion separately, for example, for each component of the protocol, these may be efficiency, scalability,

cost, and technical support. This makes it possible to simultaneously optimize various data management system protection circuits in accordance with specified target functions.

Fig. 1 shows a block diagram of the proposed approach. This diagram describes each stage of the methodology, from preliminary data processing to final evaluation and selection of the optimized model.

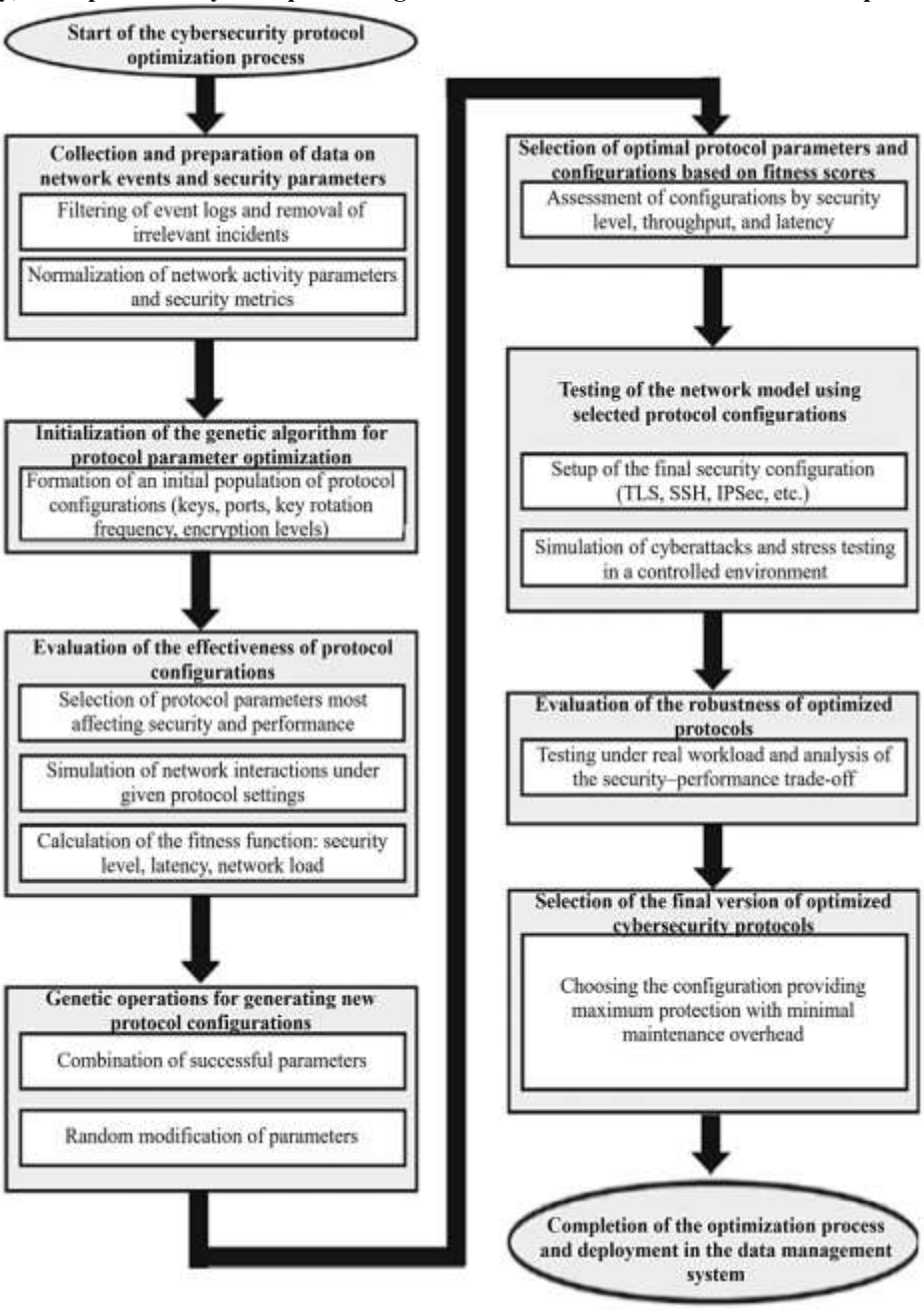

Fig. 1 Block diagram of GA use for optimising cybersecurity protocols in data management systems (compiled by the author)

So, at the first stage, it is necessary to select the objective function - W. In the context of this study, we believe that one of the main goals of optimizing cybersecurity protocols in data management systems is to improve information security metrics. In this case, we suggest choosing the probability of successful counteraction by information protection measures against all actions of the attacking party (in particular, with a possible monetary assessment) as the objective function.

To do this, we will determine the value:

$W = P^3(X) = \max_X \prod_{p_a=1}^{PA} \left(1 - \sum_{j \in G^{PA}{}_{I^{Pa}-1}} P_j^{p_a} p_{jn_{p_a}}\right)$ (1)

under restrictions: $C^q \le C_l^q$

$\sum_{j \in G^{PA}{}_{I^{Pa}-1}} P_j^{p_a} p_{jn_{p_a}} \le P_{p_a l}^{p} \quad p_a = 1,2,\dots,P$ (2)

$x_{jm} = \{0,1\}, (j \in B_{p_a}, j \ne 0; m \in N_j^{p_a}; p_a = 1,2,\dots,PA)$ (3)

where – C^q, C_l^q respectively, the base cost and maximum permissible cost of information protection protocols in data management systems; p_a – the goal of a cyber attack on data management systems; B_{p_a} - a set of cyber threats to the data management system; $P_j^{p_a}$ - the probability of attackers achieving p_a – goal; $P_{p_a l}^{p}$ - the permissible value of the probability of attackers achieving p_a – goal; $p_{jn_{p_a}} = \rho_l^{p_a} \cdot g_l^{p_a}$; $g_l^{p_a}$ – the probability of overcoming the j-th protocol when attackers attempt to achieve the p_a - goal; a $\rho_l^{p_a}$ – the probability of attackers moving to a higher level (l) in protocol states; G^{PA} - the set of data management system states when attackers attempt to achieve the attack p_a – goal; I^{Pa} – the number of levels of the data control system state graph describing the actions of attackers when attempting to achieve the p_a – goal; $N_j^{p_a}$ - the set of protocol numbers that can be used to counter the goal p_a on the j defence circuit; m – means or measures of information protection for the j-th information security circuit of data control systems.

The method of representing chromosomes has a significant impact on the efficiency of genetic search, since coding, together with the recombination operator, determines the efficiency of information exchange between populations [23]. For this task, the most optimal coding option is one in which the length of the tape is equal to the complexity of the input set and represents a bit tape, which is one of the possible solutions to the task.So, let us assume that a chromosome is a set of protective measures (for example, rules for compliance with information security policy at a protected facility), including security protocols. The set is encoded as a binary number [23, 24]. If the binary digit of the number is equal to one (1), then the corresponding protocol with the corresponding number is added to the set.

Then the range of changes in the protection contour can be represented as follows:

$G = (d_0 d_1 \dots d_{NC})_2 = (0 \dots 2NC)_{10}$ (4)

where NC is the number of available protocols that are potentially considered for inclusion in the optimal set; d_i is the inclusion of a specific protocol in the set.

In GA terms, the population will consist of instances with different chromosomes. The size of the population is limited by the maximum number of instances in it. Each instance of the population can be described as follows:

$Ch = \{G, C, R\}$ (5)

where G - the genetic code of an individual in the population; C - the cost of the corresponding protective measures; R - the total risk of information loss (or loss of confidentiality or integrity) considering the selected protocols and/or corresponding protective measures.

The next task is to select parent chromosomes. There are several approaches to selecting a parent chromosome pair. Within the framework of this study, it seems appropriate to use random selection of a parent pair from the entire population and the roulette method. The essence of the roulette method is that individuals are selected using N 'spins' of the roulette wheel, where N — the size of the population. According to this method, the selection is based on a distribution function, which is formed from the calculated values of chromosome fitness.

The mechanics of the 'roulette method' are as follows

The fitness function $F_k(X_k)$ is calculated for each chromosome X_k, $k \in (1 \dots N_{pop})$, N_{pop} – population size.

The overall fitness function for the population is determined:

$f \sum_{K=1}^{N_{pop}} F_k(X_k) - \min_{j=1,N_{pop}} (F_j(X_j))$ (6)

The probability of selection p_k is calculated for each chromosome X_k and the cumulative probability is established for each of them:

$p_k = \frac{F_k(X_k) - \min_{j=1,N_{pop}} (F_j(X_j))}{f}, k = 1 \dots N_{pop}$ (7)

The cumulative probability q_k is calculated for each chromosome X_k.

$q_k = \sum_{j=1}^{k} p_j, k = 1 \dots N_{pop}$ (8)

The selection process begins with determining the value of the vector, which is optimized N_{pop} times. At each

iteration of this step, a specific chromosome is selected in the following way: we generate a random number r_k, and if this number is less than the cumulative probability q_k of the chromosome X_k, then the k-th chromosome is selected for the next generation.
With this selection, members of the population with higher fitness will be selected more often than individuals with lower fitness [25].
So, we will write down the set of GA solutions as follows:

$$Ch = \{ch_{zt}; t = 1,2, \dots, N;\ z = 1,2, \dots, M\} \quad (9)$$

The objective function (W) is presented as a normalized additive criterion. This additive criterion should include estimates of the number of protocols designed to protect data management systems with the best information security metrics and total value, which are recommended for use:

$$W = k_1 \cdot W_1 + k_2 \cdot W_2 \quad (10)$$

where k_1, k_2 - weight coefficients for local criteria.

The weighting coefficient k_1 considers the importance of the impact of specific protocols on the overall security indicators of information management systems, while k_2 - considers the impact of the cost of an individual protocol. In addition, W_1 - is a criterion for assessing the number of protocols with low or no information security metrics, and, W_2 - is a criterion for assessing the total cost of all protocols used to protect the data management system. In other words, these are the resources needed to achieve cybersecurity goals. To solve the problem, it is necessary to maximize the value of W, i.e

$$W(Ch) \to \max(ch_{opt}) = \max(ch_{ij}),\ ch_{ij} \subset Z \quad (11)$$

In the process of modifying GA to determine the risk of security protocol violations, we use the following assumption. The absolute value of losses in monetary terms for a specific data management system depends on a chain of elements: threats, vulnerabilities, and specific protocols [26,27]. Consequently, the number of risks is the number of combinations of threats and database fragments that are confirmed by them:

$$R = TH \cdot M \quad (12)$$

where TH - the number of threats, M - the number of database fragments.
Formula (12) does not consider the combination of several threats, as well as the internal impact on cybersecurity between different protocols. Therefore, the most adequate way to determine risks is a method based on compiling attack profiles [28,29]. In this method, attack profiles are considered as sequences of attacks consisting of a combination of various threats [30]. In this case, the number of risks can be described by the following dependence:

$$R = (2^{TH})^{TA}$$

where TA – the number of attacks.
Consequently, the risk value for a given attack profile can be considered to be the total damage from successful attacks. If there is no chain reaction during the attack, the total risk value can be represented as the mathematical expectation of damage:

$$r = \sum P_{i,j} \cdot D_{i,j}, \quad i = \overline{1,TH}, \quad j = \overline{1,M}$$

where $P_{i,j}$ - probability of an information security incident caused by threat (i) to database fragment (j); $D_{i,j}$ - amount of losses associated with the incident (expressed in monetary terms).
Let's test the proposed algorithm using a specific example.
Objective: to determine the optimal set of cybersecurity protocols for protecting a corporate network and database server that maximizes the level of security within given budget constraints.

Step 1: Define input data and parameters:-
Consider four potential cybersecurity protocols (NC=4) that are planned to be implemented. Each has an implementation cost and a risk reduction indicator.Initial total risk ($R_{initial}$): 600 conventional units (monetary equivalent of potential damage). Maximum allowable budget (C_{max}): 110 conventional units.

Table 2 provides a description of the protocols and information for conducting the experiment.

Table 2 Initial data for modeling:-

№	Cybersecurity protocol	Code (d_i)	Implementation cost (Ci)	Risk reduction (ΔR_i)
1	TLS 1.3 (traffic encryption)	d_1	30	150
2	IPsec (network-level protection)	d_2	50	200
3	WPA3 (wireless network protection)	d_3	40	100
4	SSH (secure administration)	d_4	25	180

In this case, a chromosome is a binary string [d_1, d_2, d_3, d_4], representing one of the possible sets of protocols.

Step 2: Creating the initial population:-

We generate an initial population of 4 instances (sets of protocols) and calculate their cost C and total risk R (Table 3).

Table 3 Initial population and calculation parameters

Example (k)	Chromosome (G)	Protocols included	Cost (C)	Total risk (R)
1	[1, 0, 1, 0]	TLS 1.3, WPA3	70	350 (600-150-100)
2	[0, 1, 0, 1]	IPsec, SSH	75	220 (600-200-180)
3	[1, 1, 0, 1]	TLS 1.3, IPsec, SSH	105	70 (600-150-200-180)
4	[1, 1, 1, 0]	TLS 1.3, IPsec, WPA3	120	150 (600-150-200-100)

Step 3: Calculation of fitness (objective function W):-

To evaluate each instance (set of protocols), we use an objective function (W) presented in the article as a normalized additive criterion.As part of the testing, we maximize this function (W→max) with weight coefficients $\alpha_1 = 0,7$ and $\alpha_2 = 0,3$. Instance 4 is immediately rejected ($W_4 = 0$) because it exceeds the budget constraint.

Calculation of the value of the objective function W for the remaining sets:

W_1 (for TLS 1.3, WPA3) = 0,401
W_2 (for IPsec, SSH) = 0,538
W_3 (for TLS 1.3, IPsec, SSH) = 0,632

Step 4: Selection (the 'roulette method'):-

Let us calculate the selection probabilities for the next generation (see Table 4)

Table 4 Selection probabilities

Example (k)	Fitness (W_k)	Selection probability (p_k)	Cumulative probability (q_k)
1	0,401	0,255	0,255
2	0,538	0,342	0,597
3	0,632	0,402	1,0
4	0	0	1,0

The results of the testing are interpreted as follows:

1. Rejection of an unacceptable solution: the algorithm automatically rejected Example 4 because its cost exceeded the set budget, assigning it a zero fitness value.
2. Identification of the best solution in the generation: Instance 3 (a set of TLS 1.3, IPsec, and SSH protocols) showed the highest fitness ($W_3 = 0.632$) and, therefore, has the highest chances (more than 40%) of being selected to create the next generation. This set provides the lowest risk level (R=70) while complying with budget constraints.
3. Algorithm operation: in subsequent iterations, through crossover and mutation mechanisms, genes from the most fit individuals (primarily Example 3) will be combined to search for even more perfect sets of protocols.

Thus, testing demonstrates that the proposed GA effectively solves the multi-criteria problem of selecting the optimal set of cybersecurity protocols, balancing between maximizing security and minimizing costs in accordance with the specified constraints.

Conclusion:-

Artificial intelligence tools play a key role in ensuring robust cybersecurity by enabling organizations to detect threats, respond to them, and mitigate their consequences in real time. The article shows that metaheuristic algorithms and intelligent analytics offer significant advantages for improving the security of data management systems. In particular, GA are able to respond more effectively to evolving cyber threats than static systems, thanks to iterative refinement of security parameters. By reducing dependence on characteristics and processing time, these methods can be more easily integrated into real-world information systems, increasing their resilience to attacks and risks.The study presents an integrated approach that combines GAs with data analytics to optimize cybersecurity protocols in data management systems. Thanks to the dynamic adaptation of security configurations and the optimization of protocol selection, the proposed approach allows for the optimization of performance and threat detection capabilities.

As demonstrated by tests performed on a concrete example, the algorithm respects the imposed constraints and automatically eliminates solutions exceeding the allocated budget. Its main strength lies in its ability to find balanced solutions offering the best compromise between the effectiveness of data management system protection and the financial costs associated with cybersecurity.Future research should explore in greater detail hybrid models integrating genetic algorithms and deep learning to accelerate convergence and improve the accuracy of attack and vulnerability detection in information systems. Furthermore, a comparison with other evolutionary methods, such as particle swarm optimization, could confirm the effectiveness of this approach.

References:-

1. Nachaat Mohamed (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms, Knowledge and Information Systems, 67(8):6969-7055 DOI:10.1007/s10115-025-02429-y
2. Panilov P. A. (2024). Using neuroevolution methods for automating optimization of cyber security algorithms in cognitive information centers, National Security and Strategic Planning,Volume 2024, № 3. https://futurepubl.ru/en/nauka/article/95367/view
3. Anna Melman and Oleg Evsutin (2023). Efficient and error-free information hiding in the hybrid domain of digital images using metaheuristic optimization, Computer Research and Modeling, 15(1):197-210 DOI:10.20537/2076-7633-2023-15-1-197-210
4. Soodeh Hosseini, Mahdieh Khorashadizade «A Hybrid Method Using Slime Mold Algorithm and Genetic Algorithm for Feature Selection Problems in Intrusion Detection Systems». Engineering Reports, vol. 7, issue 7, 2025. https://doi.org/10.1002/eng2.70254
5. Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F., Dong, Z.Y. «Deep learning for cybersecurity in smart grids». Review and perspectives. Energy Convers. Econ, vol. 4, pp. 233–251, 2023. https://doi.org/10.1049/enc2.12091
6. Zhai J., Li Z., Miao H., Li Z., Zhou X., Yang H. «Automatic Generation of Cybersecurity Teaching Cases Using Large Language Models». Computer Applications in Engineering Education, vol. 33, 2025. https://doi.org/10.1002/cae.70081
7. Ahmad, J., Zia, M. U., Naqvi, I. H., Chattha, J. N., Butt, F. A., Huang, T., Xiang, W. «Machine learning and blockchain technologies for cybersecurity in connected vehicles». WIREs Data Mining and Knowledge Discovery, vol. 14(1), 2024. https://doi.org/10.1002/widm.1515
8. Dmitry Vasinev and Mikhail Solovev (2024). Method and Algorithm for Vulnerability Detection in the Protocols of Critical Information Infrastructure Objects, Telecom IT 12(2):1-15. DOI:10.31854/2307-1303-2024-12-2-01-15
9. Danil Klishin and Andrey Chechulin (2025). Model of the Protected Information Infrastructure for Assessing the Level of Information Security, Conference: 2025 International Russian Smart Industry Conference (SmartIndustryCon). DOI:10.1109/SmartIndustryCon65166.2025.10986155
10. Lone AN, Mustajab S, Alam M. (2023). «A comprehensive study on cybersecurity challenges and opportunities in the IoT world». Security and Privacy, vol. 6(6). DOI: 10.1002/spy2.318
11. Zeng, L., An, Y., Zhou, H., Luo, Q., Lin, Y., Zhang, Z. «A Hybrid Machine Learning-Based Data-Centric

Cybersecurity Detection in the 5G-Enabled IoT» Security and Privacy, vol. 8, 2025. https://doi.org/10.1002/spy2.472
12. Kirillova A.D., Vulfin A.M., Vasilyev V.I., Guzairov M.B.(2023). Intelligent decision support system for assessing the risks of information security violations of ICS. Modeling, Optimization and Information Technology;11(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1476 DOI:10.26102/2310-6018/2023.43.4.029
13. Sarker I.H. «Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview». Security and Privacy, vol. 17, 2023. doi:10.1002/spy2.295
14. Alsadie Deafallah (2025). Cybersecurity and Artificial Intelligence in Unmanned Aerial Vehicles: Emerging Challenges and Advanced Countermeasures». IET Information Security, vol. 5, 2025. https://doi.org/10.1049/ise2/2046868
15. Fatin A. D. (2024). Building a model of adaptability of cyber-physical systems: operation and detection, Вопросы кибербезопасности, № 2 (60), С. 36-43, 2024. vokib-2024-2-st05-s036-043.pdf DOI: 10.21681/2311-3456-2024-2-36-43
16. Heydari M., Shabgahi G. I. and Mohammad Mehdi Heydari (2013). Cryptanalysis of transposition ciphers with long key lengths using an improved genetic algorithm, World Applied Sciences Journal 21(8):1194-1199 DOI:10.5829/idosi.wasj.2013.21.8.22
17. Sarah Vluymans, Lynn D'eer, Yvan Saeys, Chris Cornelis (2015). Applications of Fuzzy Rough Set Theory in Machine Learning: : a Surv, Fundamenta Informaticae, Volume 142, Issue 1-4, pages 53 – 86 https://doi.org/10.3233/FI-2015-1284
18. Ding, S., Lu, S., Xu, Y., Korkali, M., Cao, Y. (2023). Review of cybersecurity for integrated energy systems with integration of cyber-physical systems». Energy Convers. Econ. vol. 4, pp. 334–345. https://doi.org/10.1049/enc2.12097
19. Green, M., Sarkani, S., Mazzuchi, T. «Mitigating Cybersecurity Risks in Grids With a High Penetration of Distributed Renewables». IET Cyber-Phys. Syst., vol. 10, 2025. https://doi.org/10.1049/cps2.70026
20. Fatima, Z., Hussain, R., Dilshad, A., Shakir, M., Laghari, A.A.(2025). Explainable AI-Driven Firewall Evaluation: Empowering Cybersecurity Decision-Making for Optimal Network Defense. Security and Privacy, vol. 8, 2025. https://doi.org/10.1002/spy2.70026
21. Ivan E. Chernov and Andrey V. Kurov (2022). Application of genetic algorithms in cryptography, RSUH/RGGU Bulletin Series Information Science Information Security Mathematics, № 1, С. 63-82, 2022. DOI: 10.28995/2686-679X-2022-1-63-82. Vestnik_isism_1(2022).pdf DOI:10.28995/2686-679X-2022-1-63-82
22. Dangwal, G., Wazid, M., Nizam, S., Chamola, V., Das, A.K. (2025). Automotive Cybersecurity Scheme for Intrusion Detection in CAN-Driven Artificial Intelligence of Things». Security and Privacy, vol. 8, 2025. https://doi.org/10.1002/spy2.483
23. Punitha A., Vinodha S., Karthika R. and Deepika R (2019). A Feature Reduction Intrusion Detection System using Genetic Algorithm. Conference: 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN). DOI:10.1109/ICSCAN.2019.8878704
24. Sultan H. Almotiri (2024). Improving network resilience against DDoS attacks: A fuzzy TOPSIS-based quantitative assessment approach, Heliyon 10 (22), e40413. https://doi.org/10.1016/j.heliyon.2024.e40413
25. Rohani Rohan, Debajyoti Pal, Jari Hautamäki[c], Suree Funilkul, Wichian Chutimaskul, and Himanshu Thapliyal (2023). A systematic literature review of cybersecurity scales assessing information security awareness, Heliyon 9 (3), e14234. https://doi.org/10.1016/j.heliyon.2023.e14234
26. Sanghyeop Lee, Junyeob Kim, Hyeon Kang and Do-Young Kang (2021). Genetic Algorithm Based Deep Learning Neural Network Structure and Hyperparameter Optimization, Applied Sciences 11(2). DOI:10.3390/app11020744
27. Beikbabaei, M., Mehrizi-Sani, A., Liu, C.-C. «State-of-the-art of cybersecurity in the power system: Simulation, detection, mitigation, and research gaps». IET Gener. Transm. Distrib, vol. 19, 2025. https://doi.org/10.1049/gtd2.70006
28. Zhou, Z., et al. «Comprehensive review on dynamic state estimation techniques with cybersecurity applications». IET Smart Grid, vol. 7(4), pp. 370–385, 2024. https://doi.org/10.1049/stg2.12168
29. Sharma D.M., Shandilya S.K. «An efficient cyber-physical system using hybridized enhanced support-vector machine with Ada-Boost classification algorithm». Concurrency Computat Pract Exper. vol. 34(21), 2022. DOI:10.1002/cpe.7134
30. Huang, J.-C. , et al. «SOPA-GA-CNN: synchronous optimisation of parameters and architectures by genetic algorithm with convolutional neural network blocks for securing Industrial Internet-of-Things». IET Cyber-Syst. Robot, vol. 21, 2023. https://doi.org/10.1049/csy2.12085