An Algorithmic Model Based on Optimization of the Production Rules for Phishing Attacks

Anvar Kabulov[1], Erkin Urinbaev[2], Inomjon Yarashov[3], Alisher Otakhonov[4]
National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan[1]
Sharof Rashidov Samarkand State University, Samarkand, Uzbekistan[2]
University of World Economy and Diplomacy, Tashkent, Uzbekistan[3]
Tashkent International University of Education, Tashkent, Uzbekistan[3]
Fergana State University, Fergana, Uzbekistan[4]

***Abstract*—Phishing cyber-hazards, which are a correct cyber threat to audit, monitoring, control, and data acquisition systems in the digitalization environment, are aimed at misleading participants in a complex system and editing personal digitalization data through unauthorized access. In the research work, functioning tables, production rules, algorithmic and mathematical modeling apparatus are used as a foundation for formulating, analyzing, and synthesizing the discrete adaptive behavior of large systems. In the scientific practical research work, phishing identification technologies based on production rules are implemented in solving a scientific problem by integrating access to digitalization resources into control and/or management operations and/or processes. In this research, a set of production rules is created to identify malicious and legitimate resources from URLs, URL features are extracted from a dataset of trusted platforms based on algorithmization, and logical rules are generated from these features; the authenticity of the URLs is then verified using this rule set. The results are compared with other existing models and algorithms, and two different approaches to generating production rules are developed. The study also develops a logical model for building a knowledge base from URL features and demonstrates the representation of malicious attacks through logical implications, conjunctions, and disjunctions. Finally, it tests optimized expressions based on monotone Boolean functions and their perfect disjunctive normal form (CDNF) on an independent test dataset in order to select the most efficient rule system.**

***Keywords*—Petri nets; phishing; production rules; URL; functioning table**

I. Introduction

With the development of cyberspace in the world, the rapid development of digitalization based on production rules, and the continuous development and expansion of big messages and large-scale digitalization of systems, systematic and structurization phishing cyber-hazards are among the cyber threats that affect or weaken the security measures of digitalization and complicated cyber-hazard detection systems, and the emergence of modified cyber hazards with improved attack potential is leading to combined attacks.

These production rules are proposed in the context of attempts or actions to gain unauthorized access to the structure of identification data and passwords of participants in complex cyber systems, which allows cybercriminals to gain access to highly sensitive information such as personal digital data, financial and economic digital data and other confidential communications based on unclear processing.

Phishing attacks in cyberspace are a modern trend in cyberspace, which is why a serious violation of the confidentiality of personal digital information can lead to unexpected situations, leading to the failure of the architecture of the system and significant economic and/or financial losses. The attacks are aimed at disrupting the dependability of technological procedures and/or disrupting the normal realization of intellectualization and digitalization events. In this event, it is important to guarantee that the mechanisms for controlling and/or managing permission for notes are in places are effective in combining continuous monitoring and/or auditing of security incidents, as well as to take important steps in the algorithmic design and implementation of identification systems. These complex systems can be considered a modern requirement for early detection of phishing attacks, analysis and prevention of their causes, mathematical support for stable system operation, and minimizing the negative effects that occur in complex cyber infrastructures. The identification mechanisms developed in the next step form the scientific and practical basis for the application of simulating and imitation instruments used to evaluate, optimize, and validate key security solutions at the algorithmic design stage before their practical application.

Algorithmic modeling and algorithmization in cyberspace are the expression of security tasks for algorithmic design in modern information protection, the formal basis of protection logic in digital computing systems operations, the optimization of production rules describing system states, events and corresponding security responses, the algorithmization process for phishing-related threats, the decomposition of complicated anti-phishing tasks into elementary functional items, the organization of items into security solutions application of parallel events, synchronization, imitation modeling scientific ways, the generation of optimized rule-based imitation models, the generation of flexible, resilient anti-phishing protection systems, the possibility of visualizing system behavior in various attack scenarios in real cyber environments, supporting simulation and verification procedures.

One of the comprehensive elements with a wide range of coverage for simulating and synthesizing, and analyzing complicated cyber hazards detection systems is a functioning table. It composites ways to structural, graphical, mathematical

and systematic simulating, ensuring a correct definition of adaptive events. The functioning table not only applies as a fundamental for synthesizing the act of permission management structures, but also contributes to the algorithmic simulation or structuring of missions in combination with their construction and development of settings [13, 14].

Composing algorithmic simulating, imitation, and mathematical techniques enables contemporary probability frameworks to generate fixed and highly successful anti-phishing cybersecurity solutions. These actions highlight the importance of joining fundamental structures, conceptual details, and empirical technologies to supply reliable cybersecurity.

II. Related Works

The dangers of phishing are becoming an increasingly crucial cybersecurity risk, and more research and experiments are focused on constructing techniques to detect, identify, and prevent them. In this context, Petri nets have proven to be a vital tool for simulating, evaluating, and assessing cyberspace-related structures and substructures, such as those related to permission control and/or access control, cybersecurity, and/or information security [10]. This analytical and structural review of scientific and academic sources systematically analyzes and synthesizes various practical-fundamental approaches and ways to implement the identification of cybersecurity [11] sensitive features in cyberspace in a fundamental and innovative way, including the practical and innovative application of Petri nets. Mathematical and logical-algebraic simulation technological methods, along with structural and functional structural analysis or synthesis, are considered to play a key role in the investigation of the mechanisms of sustainable resilience, adaptability, dynamics, management, control and regulation of systems or structures, and the identification and determination of effective strategic actions to reduce the risks of phishing in the structural and structural elements of the system [15]. The fundamental experimental research conducted by Yu, Wangyan, and colleagues (2024) achieves this goal by synthesizing the innovative fundamental application of dynamic adaptive optimal decomposition and colored Petri nets (CPN) in the structural systems of electronic toll collection in digital computing environments installed in cyberspace. In the context of innovative adaptation to the progressively developing implementation characteristics of cyber threats, such as the behavior of phishing attacks in cyberspace, applied-fundamental research supports the demonstration of the practical potential of Petri nets in the formation of descriptions of complex composite structural systems, in which the main fundamental-innovative operations include mathematical logic, adaptively adapting to the dynamic behavior and algorithmic state of implementation. This innovative-fundamental approach technology combines the graphical representation of mathematical networks with the technical practice of dynamic and adaptive decomposition in a modern digital society, which supports the possibility of validating the systematic robustness of a system capable of self-development in various virtual and digital environments. The resulting part of the study supports the understanding of the research mechanisms used in the implementation and identification of potential cyberspace threats based on a deeper synthesis of the current state of the art. Gelen and İçmez (2024) suggest a Petri net-based treatment for task planning and legal administration of robotic assembly structures [16]. The scientific-fundamental approach to cyberspace research can be significantly expanded to support the implementation of systematic, analytical, automated systematic digitization of composite and combined threats that are considered harmful to the nuclear sphere of cybersecurity, such as phishing, in the form of identification and synthesis of responses. It is experimentally proven that when a threat is detected in cyberspace, the system can be established and adjusted using mathematical tools, maintaining the sequence of each step, while maintaining a consistent and logical connection of each step. Such a research method steadily monotonically increases the structurally generalized complex strength of the system and reduces the probability of successful phishing cyberattacks in cyberspace, which have significant practical damage in practice and are studied [1].

To determine the resilience of access management structures, Yang and Hu (2024) study role-based access control (RBAC) and restriction enforcement [17]. Researchers are performing research analysis and synthesis with the aim of providing the ability to implement Petri nets in mathematical logic as well as fundamental mathematical programming, in order to demonstrate that such structured systems can withstand various cyberthreats in cyberspace, such as phishing cyberattacks, while maintaining their adaptiveness. Here, the scientific research work provides support for the algorithmic implementation of complex logical strict constraints that restrict access and permissions to confidential data within the structured system, only to authorized participants, which is an algorithmic logical critical measure for identifying and protecting against cyber threats with complex phishing dependencies occurring in cyberspace.

Liu (2024) studies the opacity testing of archival structures utilizing constrained Petri net labels, which is relevant for providing that sensitive messages in archival structures are protected from unauthorized access. This innovative scientific research specifically applies the correct sequence of actions to malicious phishing and composite threats in cyberspace that attempt to trick participants in a structured system into disclosing mathematically-based authentication digital information to control access to electronic business data resources or stored confidential data repositories [18].

Anguiano-Gijón et al. (2024) scientifically study a series of algorithmic regulations and regulative management strategies based on Petri nets, while preserving the mathematical essence of their implementation in complex automated information systems in cyberspace [19]. Their scientific and innovative research introduces a scientific and innovative approach to the implementation of dynamic regulatory management mechanisms capable of monitoring the complex state of the system and responding to potential threats in cyberspace in an efficient and algorithmic manner.

The use of Petri nets to imitate cyber-hazards is extended by Petty et al (2024), who ensure practical instruments for imitating the dynamics of phishing and other forms of adversarial action [20]. Innovative-fundamental research can be aimed at improving Petri nets in a logical sequence, optimally minimizing

the development of systems with structural performance capabilities that perform proactive and active protection measures against phishing in cyberspace, using innovative-mathematical methods, cyclically repeating the progressive spread of cyberthreats and, in this case, supporting the empirical assessment of the effective impact on the functions of the generalized structural system [2].

Yang et al (2024) investigate a dynamic or adaptive Petri net-based approach to structure message safety [21]. The authors' collective ideological idea is that the identification systems of cybersecurity threats based on Petri nets using mathematical tools can effectively and rationally solve phishing and other complex cyber threats with minimal effort in the digital and cyberspace environment, while maintaining the inherent, self-algorithmic nature of cyberspace, and achieve a sufficiently progressive level of scientific and innovative development. In this context, there is a strong need for methods of structural protection of communication in real time, which are stable in dynamic changes depending on the conditions, without violating the sequence, while maintaining the sequence. Scientific and innovative research shows that modern digital security models need to be in a sequence of flexible and adaptive control in cyberspace, which supports them in identifying and reactively responding to fundamentally progressive phishing identification and attack techniques [3].

The reliability and robustness of intelligent digital transport automated structural systems in cyberspace have been scientifically and innovatively studied using the important generalized stochastic Petri nets in empirical studies. This technological method provides a sequence of concepts for the algorithmic development and adaptive control of complex cyber threats [7-9] that cause damage to cyberspace, such as phishing and trust-based cyberattacks with a strong damage domain. In the era of the digital economy, it emphasizes the need for systems to dynamically self-adjust to optimally respond to threats effectively by analyzing and/or synthesizing multiple cyberspace cyber threat scenarios [4-6].

III. Problem Statement

In the modern cyberspace environment, the progressive increase in the volume of data and the complexity of the algorithmic nature of the structured system in digital security and ecosystems has systematically increased the level of phishing cyber-risk in terms of the importance of digitization, which creates a significant optimization in the regulation of the infrastructure for protecting and eliminating risks, auditing, monitoring and managing complex structured confidential information. The foundation of cyber-hazards in this category of cyberspace is aimed at generating the ability of legitimate structure participants to gain unauthorized permission and bypass the authentication event, in an algorithmic sequential manner based on event imitation and architectural analysis, allowing attackers to gain unauthorized access to confidential digital data that should be kept confidential, such as personal and/or financial data. The algorithmic nature of digital data corruption, operational disruptions, and structural duplications, and widespread financial losses often result in operational failures and structural duplications, highlighting the importance of robust cyberspace defense strategies and approaches that operate reactively.

In order to create immunity to cyberspace threats, modern web systems include the ability to detect sensitive phishing in cyberspace in an algorithmic manner directly into authorization and access control systems. In such a situation, it is appropriate to implement comprehensive and multi-criteria modeling and technological tools that are based on the fundamental basis of functional table-graph, structural, algorithmic, logical, and mathematical theories. The fundamental basis for the digital representation of complex structural systems in cyberspace in a coordinate system is generated, which allows for the analysis and synthesis of dynamic events in adaptive conditions, which is involved in the regulatory management and control of digital security.

Building effective, optimized, and reactive anti-phishing mechanisms relies on a sophisticated, structured algorithmic approach to access control and digital security auditing and monitoring procedures in cyberspace. This sophisticated, structured approach supports early detection of malicious algorithmic activity, progressively reduces the negative impact on complex systems in cyberspace, and supports simulation and modeling technology in the structural design of algorithmic digital protection solutions. Algorithmic modeling and algorithmization are essential for creating reliable cybersecurity solutions between the theoretical problem description and the practical-innovative implementation of abstract security problems into clearly defined algorithmic computational stages. The versatile analytical tool, the functional table, shows the possibility of evaluating and configuring access control systems by accurately recording their dynamic behavior, and its application in cybersecurity research is based on dynamic system analysis and mathematical modeling, as well as algorithmic sequencing of phishing attacks in advanced digital environments.

IV. Architecture and Mathematical Formalization of the Research Process

Our chosen dataset is https://gregavrbancic.github.io/Phishing-Dataset/. Fig. 1 illustrates the architecture for detecting or identifying phishing attacks based on the digital informational features of suspicious web-links, which consists of several main stages. First, web page data is collected, and then important informational features are extracted from the digital information in these pixels. The extracted digital features are analyzed and synthesized using algorithms to classify the web link as “trustworthy” or “phishing”.

This cycle usually consists of several stages. Initially, the attacker creates a fake website or deceptive content, and then these fake web resources are distributed to users through communication channels, causing system participants to believe the messages. When they click on fake links, after being redirected to a fake web link, the attacker obtains this information and uses it for illegal purposes (see Fig. 2).

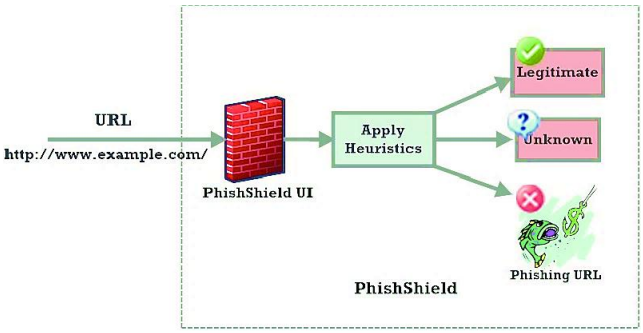

Fig. 1. A structural framework for identifying phishing attacks using visual characteristics extracted from suspicious websites [22].

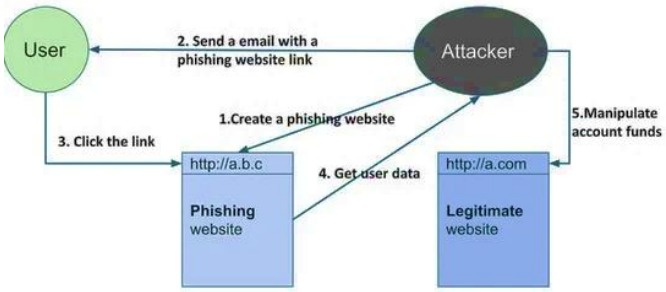

Fig. 2. The sequential stages illustrating the life cycle of a phishing attack [22].

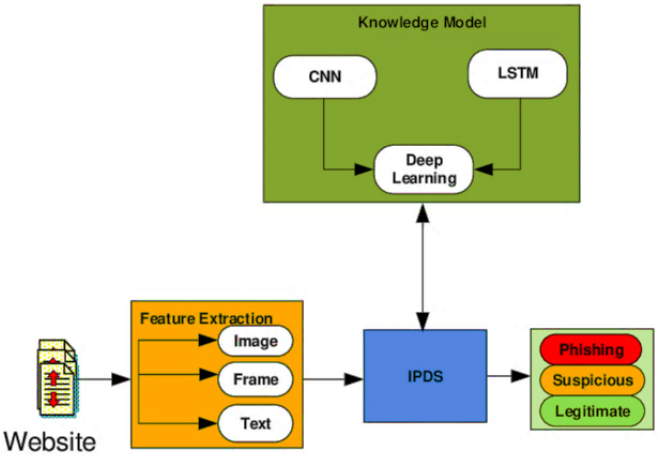

Fig. 3. The architectural design of the intelligent phishing detection system (IPDS) [22].

This structure consists of several components in an interconnected cyberspace environment, where, in the initial stage, incoming digital data is collected from various sources (websites, URLs, user queries, and other data). In this cyberspace, the digital data is pre-processed, and important informative features and extracted informative features are transferred to a knowledge base, where, based on pre-formed production rules and experience, the system's inference mechanism makes a decision to classify a website or link as "safe" or "phishing" based on the available knowledge (see Fig. 3).

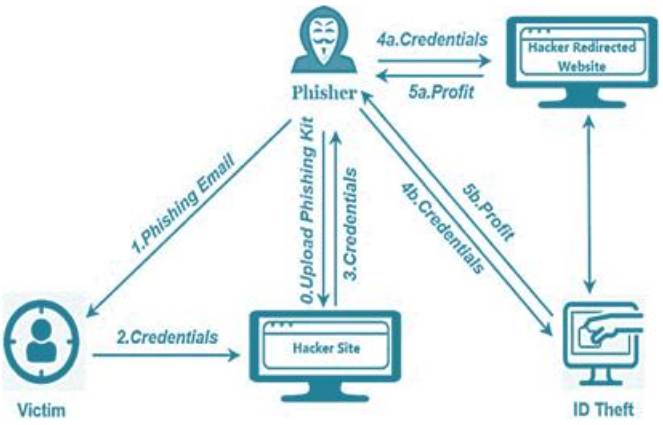

Fig. 4. Phishing attack diagram [22].

The phishing attack involves the attacker and the system participant entering confidential digital information to redirect to a fake web page by clicking on a link. The attacker uses this digital information for illegal purposes in the last part of the diagram. This usually involves an attacker creating a fake website or service that looks very similar to the original site, intended to mislead the intended user (Fig. 4).

The functioning table is represented through a formal mathematical framework [24, 36, 37]:

$$FT = (P, T, F, W, \mu_0, F_x, F_y)$$

where,

- P: a finite set of places
- T: a finite set of transitions
- F: a set of directed arcs connecting places and transitions
- W: a weight function that assigns positive integer values to arcs
- μ_0: the initial distribution of tokens across the places
- F_x: a set of coordinates corresponding to the x-axis of the functioning table
- F_y: a set of coordinates corresponding to the y-axis of the functioning table.

In the simulation of coordinated actions in cyberspace, the dynamic behavior of the functional table is regulated by the transition rules and a validation procedure is performed. In cyberspace, the transition is activated in the active state when all the input points satisfy the necessary and sufficient conditions. Once these necessary and sufficient conditions are met in the environment, the transition from the point of view of digitization begins in a sequential manner, where the subsequent algorithmic essence of the tokens leads to the movement (or generation) of positions (Table I and Table II). To activate this phenomenon in an algorithmic structural way, the procedure is performed to ensure the progressive development of the states within the system when there is a real number of input function positions [26, 27].

TABLE I. POSITIONS (P)

№	Positions(p)	Description
1	p_1	Login request has been initiated
2	p_2	Phishing analysis has been carried out
3	p_3	A phishing attempt has been identified
4	p_4	No phishing activity has been found
5	p_5	The authentication process is in progress
6	p_6	User authentication has been successfully completed
7	p_7	Authentication attempt has failed
8	p_8	Access has been approved
9	p_9	Permission rejected

TABLE II. TRANSITIONS (T)

№	Transitions(t)	Description
1	t_1	The user initiates the process by submitting a request to log into the system.
2	t_2	At the same time, the procedure for detecting potential phishing activity is activated.
3	t_3	If any suspicious phishing-related indicators are identified, the system flags them accordingly.
4	t_4	On the other hand, if no signs of phishing or malicious behavior are found, this is also confirmed by the system.
5	t_5	Following this, the authentication phase begins.
6	t_6	The system carefully examines and validates the provided login credentials.
7	t_7	In cases where the credentials are incorrect or do not match the stored data, access is denied and an error is returned.
8	t_8	However, if all the entered information is accurate and successfully verified, the user is granted access to the system.
9	t_9	Ultimately, the system either approves the login attempt by granting permission or rejects it by denying access.

Incident Matrix:

$$W^- = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \\ p_8 \\ p_9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \quad (1)$$

$$W^+ = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \\ p_8 \\ p_9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \quad (2)$$

$$W^T = W^+ - W^- \quad (3)$$

$$W^T = \begin{array}{c} \\ p_1 \\ p_2 \\ p_3 \\ p_4 \\ p_5 \\ p_6 \\ p_7 \\ p_8 \\ p_9 \end{array} \begin{array}{c} \begin{array}{ccccccccc} t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 \end{array} \\ \begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array} \quad (4)$$

V. EXPERIMENTAL RESULTS

The presented scientific-innovative research work creates a number of innovative structural experimental findings that confirm the mathematical reliability and algorithmic consistency of the algorithmic model of regulatory management and/or regulatory control of permissions and access in a structural manner [12]. The functional table is built around the basis of mathematical logic and algebra, and the algorithmic nature of the mechanisms of detection and identification of phishing attacks in cyberspace is comprehensively evaluated by the model. The analysis and synthesis of the results showed that the algorithmic design approach works in a mathematically reliable implementation in cyberspace in a series of virtual digital conditions that have undergone a series of experimental tests, where the structural effectiveness of the algorithmic sequence in detecting attempts of algorithmic nature, such as phishing, is confirmed, while supporting a digitally secure and permission-controlled access to the structural system (see Fig. 5)[28, 30].

$$\begin{gathered} \mu_1 = (1\,0\,0\,0\,0\,0\,0\,0\,0) \\ \downarrow t_2 \\ \mu_2 = (0\,1\,0\,0\,0\,0\,0\,0\,0) \\ \downarrow t_3 \\ \mu_3 = (0\,0\,1\,1\,0\,0\,0\,0\,0) \\ \downarrow t_4, t_7 \\ \mu_4 = (0\,0\,0\,0\,1\,0\,1\,0\,0) \\ \downarrow t_5, t_9 \\ \mu_5 = (0\,0\,0\,0\,0\,1\,0\,0\,1) \\ \downarrow t_6 \\ \mu_6 = (0\,0\,0\,0\,0\,0\,0\,1\,1) \end{gathered} \quad (5)$$

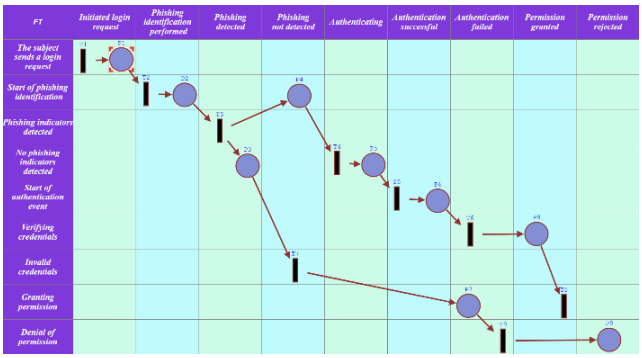

Fig. 5. The initial status of designing the imitation model based on the fundamental principles of the functioning table.

The fundamental algorithmic challenge in the functional table is to accurately represent the structural changes between the coordination links of positions and transitions in cyberspace, as well as the algorithmic nature of the transitions to positions in a precise sequence [38, 39]. This complex task involves the implementation of a validation check of the algorithmic and structural consistency and structural correctness of the dynamic changes of the state in a fundamentally sound situation. This is achieved by applying the supported feasibility analysis and synthesis, which are introduced to systematically verify the algorithmic stability, structural accuracy, and mathematical reliability of the constructed algorithmic model [34, 35] (see Fig. 6 to Fig. 11).

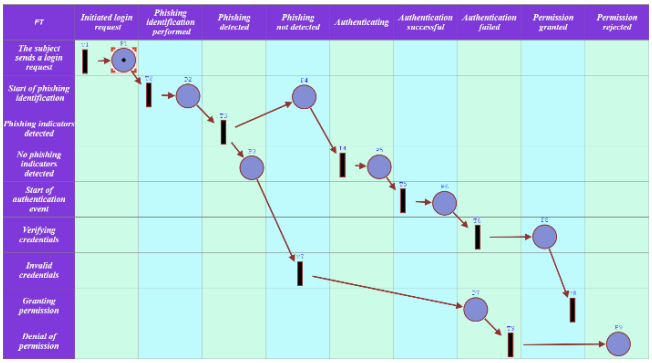

Fig. 6. $\mu_1 = (1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$ status of designing the imitation model based on the fundamental principles of the functioning table.

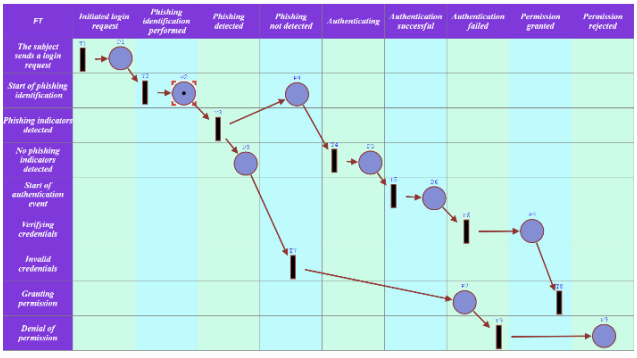

Fig. 7. $\mu_2 = (0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0)$ status of designing the imitation model based on the fundamental principles of the functioning table.

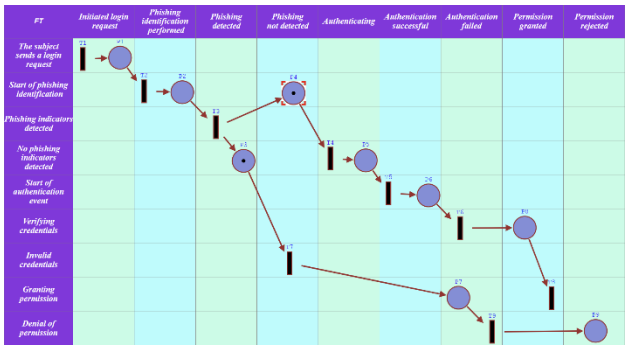

Fig. 8. $\mu_3 = (0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 0)$ status of designing the imitation model based on the fundamental principles of the functioning table.

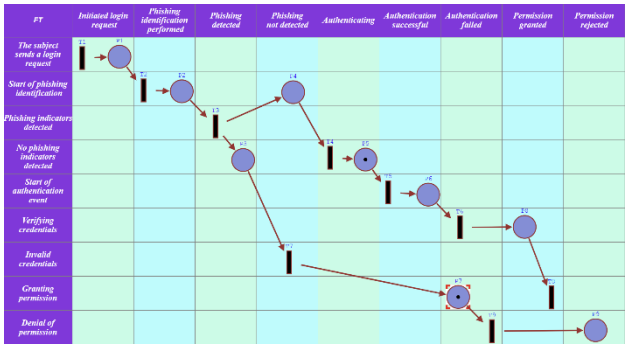

Fig. 9. $\mu_4 = (0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0)$ status of designing the imitation model based on the fundamental principles of the functioning table.

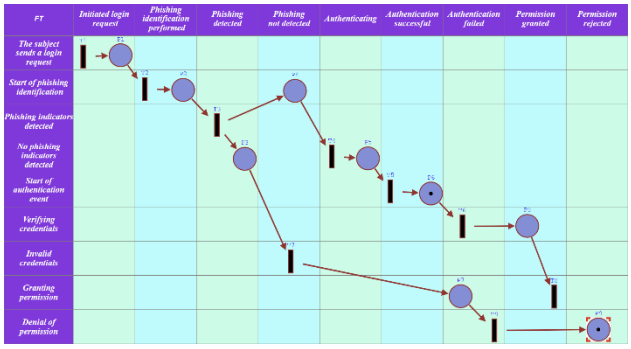

Fig. 10. $\mu_5 = (0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 1)$ status of designing the imitation model based on the fundamental principles of the functioning table.

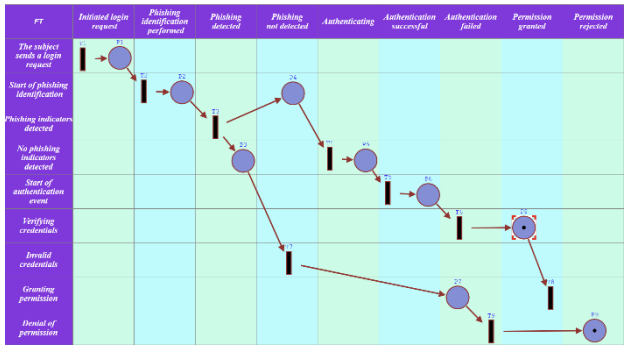

Fig. 11. $\mu_6 = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1)$ status of designing the imitation model based on the fundamental principles of the functioning table.

To generate a production rule set, URL features are extracted from datasets recorded from trusted platforms. Using the extracted features, a production rule set is generated. Based on these rules, the URL dataset is checked for authenticity or falsification. Verification results of other studied models and algorithm results are compared.

We propose two approaches to generating rules based on URL features. In approach 1, a set of rules is generated based on each of the N datasets. Then, the generated N sets of rules are combined. Using the generated set of rules, the N datasets are checked for authenticity or falsity. As a result of the verification, the rules that performed best in each dataset are combined to generate a final set of rules. A visual representation of this approach is shown in Fig. 12.

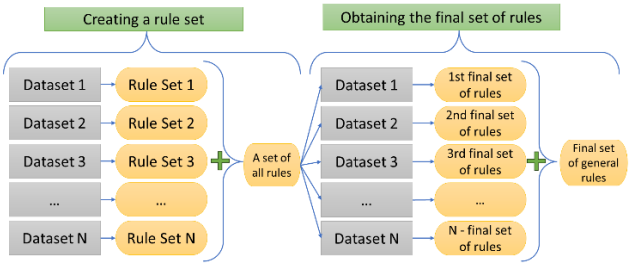

Fig. 12. Approach 1 for generating a rule set.

In approach 2, the remaining datasets are checked for real or fake URLs based on the rule sets generated from each of the N datasets. After checking, the rules in each dataset that achieve high performance are extracted. These rules form the final overall rule set. A visual representation of this approach 2 is shown in Fig. 13.

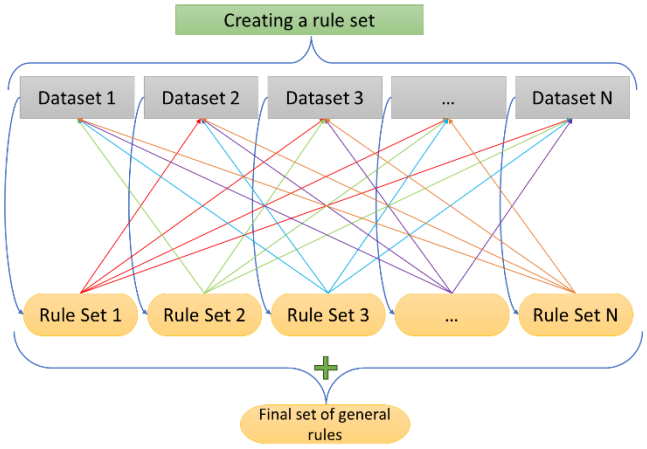

Fig. 13. Approach 2 for generating a rule set.

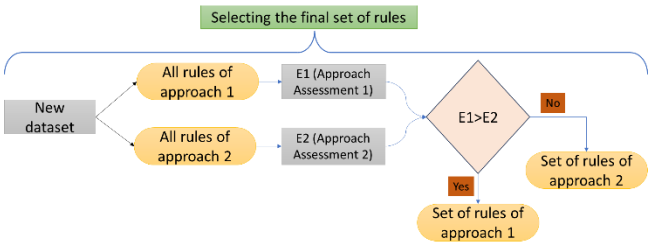

Fig. 14. Structure of building a knowledge base of URL features.

The final step of our proposed method is to test a completely different URL dataset using both approaches. The set of rules that performs best is selected.

In the digital era and digital economy, information and communication digitization technologies have been deeply embedded in almost all fundamental scientific aspects of everyday life in a comprehensive algorithmic sequence (Fig. 14). The progressive rapid development of digital technologies in this cyberspace coordination creates a large-scale opportunity to solve algorithmic problems of cybersecurity in important objects such as digitized diplomacy and medicine, logical problems related to the structural processing of large-scale digital data and algorithmic regulatory management and control. In the digitalization environment, data collection, processing, algorithmic analysis and synthesis directly affect the overall level of security in cyberspace [25]. It is necessary to conduct in-depth research on the coordination of cyberattacks in cyberspace and conduct experimental analytical studies. In this context, the production logic knowledge base for identifying and classifying specific structural categories of cyberthreats in algorithmization is examined algebraically and systematically [29,31]. Here, the corresponding algebraic logical functions can be expressed in a formalized form in the elements of mathematical logic:

$$(X_i \to Y) \equiv 1, \quad i = \overline{1,n}$$

$$\left((X_i \wedge X_j) \to Y\right) \equiv 1, \quad i,j = \overline{1,n}, i \neq j$$

$$\left((X_i \wedge X_j \wedge X_k) \to Y\right) \equiv 1, \quad i,j,k = \overline{1,n}, i \neq j \neq k$$

$$\left((X_{i_1} \wedge X_{i_2} \wedge \cdots \wedge X_{i_k}) \to Y\right) \equiv 1, \quad i_1, i_2, \ldots, i_k = \overline{1,n}, i_1 \neq i_2 \neq \cdots \neq i_k, 1 \leq k \leq n$$

$$\left((X_1 \vee X_2 \vee X_n) \to Y\right) \equiv 1$$

$$\left((X_i \vee X_j) \to Y\right) \equiv 1, \quad i,j = \overline{1,n}, i \neq j$$

$$\left((X_i \vee X_j \vee X_k) \to Y\right) \equiv 1, \quad i,j,k = \overline{1,n}, i \neq j \neq k$$

$$\left((X_{i_1} \vee X_{i_2} \vee \cdots \vee X_{i_k}) \to Y\right) \equiv 1, \quad i_1, i_2, \ldots, i_k = \overline{1,n}, i_1 \neq i_2 \neq \cdots \neq i_k, 1 < k < n$$

$$\left((X_1 \vee X_2 \vee \cdots \vee X_n) \to Y\right) \equiv 1$$

In the modern era of development, it is important to research, synthesize and algorithmically analyze cybersecurity issues on a scientific and innovation basis. This includes developing plans to safe cyberattacks on critical information infrastructure facilities and their direct implementation, regulating the activities of cybersecurity agencies, independent special services and teams, interacting with right enforcement agencies in the field of combating cyberthreats, and informing status and financial management bodies [23]. One of the fundamental basic problems of cybersecurity is identification, and application of Production Logic [32,33]. You are able to define a cyber-hazard in the formalization of algebraic-logical functions:

$$F1 = x_1 \wedge \overline{x_2} \wedge \overline{x_3} \wedge \overline{x_4} \wedge x_5 \wedge \overline{x_6} \wedge \overline{x_7} \wedge x_8 \wedge x_9 \vee x_1 \wedge \overline{x_2} \wedge \overline{x_3} \wedge \overline{x_4} \wedge x_5 \wedge \overline{x_6} \wedge x_7 \wedge \overline{x_8} \wedge \overline{x_9} \vee$$

$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge\overline{x_6}\wedge x_7\wedge\overline{x_8}\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge\overline{x_6}\wedge x_7\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge\overline{x_6}\wedge x_7\wedge x_8\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge\overline{x_8}\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge\overline{x_8}\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge x_8\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge x_7\wedge\overline{x_8}\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge x_7\wedge\overline{x_8}\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge x_7\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge\overline{x_4}\wedge x_5\wedge x_6\wedge x_7\wedge x_8\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge x_4\wedge\overline{x_5}\wedge\overline{x_6}\wedge\overline{x_7}\wedge\overline{x_8}\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge x_4\wedge\overline{x_5}\wedge\overline{x_6}\wedge\overline{x_7}\wedge\overline{x_8}\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge x_4\wedge\overline{x_5}\wedge\overline{x_6}\wedge\overline{x_7}\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge x_4\wedge\overline{x_5}\wedge\overline{x_6}\wedge\overline{x_7}\wedge x_8\wedge x_9\vee x_1\wedge\overline{x_2}\wedge\overline{x_3}\wedge x_4\wedge\overline{x_5}\wedge\overline{x_6}\wedge x_7\wedge\overline{x_8}\wedge\overline{x_9}\vee\ldots\vee$$
$$\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge\overline{x_6}\wedge x_7\wedge x_8\wedge x_9\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge\overline{x_8}\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge\overline{x_8}\wedge x_9\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge\overline{x_7}\wedge x_8\wedge x_9\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge x_7\wedge\overline{x_8}\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge x_7\wedge\overline{x_8}\wedge x_9\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge x_7\wedge x_8\wedge\overline{x_9}\vee$$
$$\vee x_1\wedge x_2\wedge x_3\wedge x_4\wedge x_5\wedge x_6\wedge x_7\wedge x_8\wedge x_9.$$

E_n^2- to the cube $n-k$ we get a cube of the size of a part. E_{n-k}^2 in this cube $\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_k}\in\{0,1\}$ and they are invariant, $E_{n-k}^2(\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_k})$the vector vertices are formed according to the remaining coordinates. $|E_{n-k}^2|-$ we obtain an invariant three-dimensional vector interval. Here $(\beta_1,\beta_2,\ldots,\beta_n),\beta_i\in\{0,1,2\},i=1,2,\ldots,n$; $\beta_{i_1}=\alpha_{i_1},\beta_{i_2}=\alpha_{i_2},\ldots,\beta_{i_k}=\alpha_{i_k}$, the remaining β_i ones are equal to 2. We write an elementary conjunction corresponding to this interval:

$$x_{i_1}^{\alpha_{i_1}},x_{i_2}^{\alpha_{i_2}},\ldots,x_{i_k}^{\alpha_{i_k}}$$

This elementary conjunction $E_{n-k}^2(\alpha_{i_1},\alpha_{i_2},\ldots,\alpha_{i_k})$ corresponds to the vector vertices of the partial cube.

$F1$ domain of the function is E_{13}^2 the cube of (1,2,2,2,2,2,2,1,1,1,2,2,2), (1,2,2,2,2,2,2,1,1,2,1,2,2), (1,1,2,2,2,2,2,2,2,2,2,2,2), (1,2,1,2,2,2,2,2,2,2,2,2,2), (1,2,2,1,2,2,2,2,2,2,2,2,2), (1,2,2,2,1,2,2,2,2,2,2,2,2), (1,2,2,2,2,1,2,2,2,2,2,2,2), (1,2,2,2,2,2,1,2,2,2,2,2,2) corresponds to the vector nodes of the cube of the part. $F1$ CDNF (complex disjunctive normal form) form of the function is given in the space E_{13}^2, the first interval of the cube corresponds (1,2,2,2,2,2,2,1,1,1,2,2,2) to $x_1\wedge x_8\wedge x_9\wedge x_{10}$the conjunction, the second interval (1,2,2,2,2,2,2,1,1,2,1,2,2) to the conjunction (1,1,2,2,2,2,2,2,2,2,2,2,2), the third $x_1\wedge x_8\wedge x_9\wedge x_{11}$ interval to the conjunction, (1,2,1,2,2,2,2,2,2,2,2,2,2) the $x_1\wedge x_2$ fourth $x_1\wedge x_3$ interval (1,2,2,1,2,2,2,2,2,2,2,2,2) to $x_1\wedge x_4$ the conjunction, the fifth interval (1,2,2,2,1,2,2,2,2,2,2,2,2) to the $x_1\wedge x_5$ conjunction, the sixth interval to the conjunction, the seventh interval (1,2,2,2,2,2,1,2,2,2,2,2,2) to $x_1\wedge x_6$ the conjunction, and the eighth interval (1,2,2,2,2,2,2,1,2,2,2,2,2) to $x_1\wedge x_7$the conjunction.

It is known that, $F1$, the function corresponds to a monotone Boolean function and its optimized form is:

$$F1=x_1\wedge x_8\wedge x_9\wedge x_{10}\vee x_1\wedge x_8\wedge x_9\wedge x_{11}\vee x_1\wedge x_2\vee x_1\wedge x_3\vee x_1\wedge x_4\vee x_1\wedge x_5\vee x_1\wedge x_6\vee x_1\wedge x_7.$$

In this research work, the optimization of Boolean functions serves to improve the inference mechanism using minimal classical Boolean functions for existing algorithms, while the formalization of the knowledge base based on production logic is important for the exploration of the dataset with localization, the formalization of the general knowledge base and the modeling of phishing attacks and identification processes using the Functioning table is important for the analysis and synthesis of dynamic characteristics compared with existing researches, and the integration with systems operating in dynamic and real modes is realized.

VI. Conclusion and Future Work

With the growing volume of data in cyberspace, combating phishing attacks will become a key challenge in ensuring cybersecurity in complicated cyberspace identification systems, as phishing cyber-hazards violate the confidentiality of digital data, disrupt system operations, and subsequently lead to significant economic losses. Therefore, this study developed a set of rules for identifying malicious and legitimate resources based on URLs. Using algorithms, URL characteristics were extracted from a dataset of trusted platforms, and logical rules were generated based on these characteristics. The authenticity of URLs was then verified using this set of rules, and the results were compared with other existing models and algorithms, resulting in two different approaches to generating inference rules. This study developed a logical model for constructing a knowledge base based on URL characteristics and demonstrated the representation of malicious attacks through logical implications, conjunctions, and disjunctions. The program tests optimized expressions based on monotone Boolean functions and their perfect disjunctive normal form (CDNF) on an independent test dataset to select the most effective rule system. Using function tables and algorithmic modeling, it enables efficient generation, analysis, and development of solutions to protect systems from phishing attacks. The most important contribution of the research work is the novelty of bringing it to the form of production rules and thereby reducing the complexity of the algorithm by reducing the informative features. Ultimately, it proves to provide an accelerated response in detecting and filtering phishing.

References

[1] Blaga, F. S., Pop, A., Hule, V., & Indre, C. I. (2021). The efficiency of modeling and simulation of manufacturing systems using petri nets. IOP Conference Series.Materials Science and Engineering, 1169(1) doi:https://doi.org/10.1088/1757-899X/1169/1/012005

[2] Trevor, R., Beckett, S., & Jevtić Petar. (2025). The basic reproduction number for petri net models: A next-generation matrix approach. Applied Sciences, 15(23), 12827. doi:https://doi.org/10.3390/app152312827

[3] Horváth, Á., & Molnár, A. (2022). TiPeNeSS: A timed petri net simulator software with generally distributed firing delays. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 3(8), e3. doi:https://doi.org/10.4108/eai.24-8-2015.2261343

[4] Kabulov, A.; Babadzhanov, A.; Baizhumanov, A.; Saymanov, I.; Babadjanov, A. Algorithms for Solving Systems of Boolean Equations Based on the Transformation of Logical Expressions. Mathematics 2026, 14, 594. https://doi.org/10.3390/math14040594

[5] Kabulov, A.; Normatov, I.; Saymanov, I.; Baizhumanov, A. On the Completeness of Classes of Correcting Functions of Heuristic Algorithms, Azerbaijan Journal of Mathematics, 2025, vol 15, no. 2. https://doi.org/10.59849/2218-6816.2025.2.51

[6] Kabulov, A.; Baizhumanov, A.; Saymanov, I. Synthesis of Optimal Correction Functions in the Class of Disjunctive Normal Forms. Mathematics 2024, 12(13), 2120. https://doi.org/10.3390/math12132120

[7] Saymanov, I., Eshkuvatov, Z., Khayrullaev, D., & Nurillaev, M. (2025). Improvement in volterra-fredholm integro-differential equations by

adomian decomposition method. Journal of Mathematics, Mechanics and Computer Science, 128(4), 92–107. https://doi.org/10.26577/JMMCS202512847

[8] Islambek Saymanov et al. AI-Based OTDR Event Detection, Classification and Localization in Optical Communication Networks. Advances in Artificial Intelligence and Machine Learning. 2025;5(4):257. https://dx.doi.org/10.54364/AAIML.2025.54257

[9] Sun, Q.; Wei, Sh.; Saymanov, I.; Lu, Y. Deng, W.; Lou, J. A Mechanical–Electrical Damage Model for Performance Analysis of Crack-based Strain Sensor. Int. J. Appl. Mech. 2026, 18(1), 2550124. https://doi.org/10.1142/S1758825125501248

[10] Kabulov, A., Baizhumanov, A., Berdimurodov, M. (2024). On the minimization of k-valued logic functions in the class of disjunctive normal forms. Journal of Mathematics, Mechanics and Computer Science, 121(1), 37–45. https://doi.org/10.26577/JMMCS202412114

[11] Islambek Saymanov, et al. Numerical Methods of Synthesis of a Correct Algorithm for Solving Recognition Problems. Advances in Artificial Intelligence and Machine Learning. 2025;5(1):202. https://dx.doi.org/10.54364/AAIML.2025.51202

[12] A. Kabulov, I. Normatov, E. Urunbaev and F. Muhammadiev, "Invariant Continuation of Discrete Multi-Valued Functions and Their Implementation," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-6, doi: 10.1109/IEMTRONICS52119.2021.9422486.

[13] Abdul Hameed, M. S., Sofiene, L., & Andreas, S. (2025). Learnable petri net neural network using max-plus algebra. Machine Learning and Knowledge Extraction, 7(3), 100. doi:https://doi.org/10.3390/make7030100

[14] Hybrid weighted fuzzy production rule extraction utilizing modified harmony search and BPNN. (2025). Scientific Reports (Nature Publisher Group), 15(1), 11012. doi:https://doi.org/10.1038/s41598-025-95406-y

[15] Yu, Wangyang, et al. "Modeling and Analysis of ETC Control System with Colored Petri Net and Dynamic Slicing." ACM Transactions on Embedded Computing Systems 23.1 (2024): 1-27.

[16] Gelen, Gökhan, and Yasemin İçmez. "Task planning and formal control of robotic assembly systems: a petri net-based approach." Ain Shams Engineering Journal 15.7 (2024): 102804.

[17] Yang, Benyuan, and Hesuan Hu. "Resiliency Analysis of Role-Based Access Control via Constraint Enforcement and Mathematical Programming." IEEE Transactions on Systems, Man, and Cybernetics: Systems (2024).

[18] Liu, Zhenzhong. "Verification of archive system opacity with bounded labeled petri nets." IEEE Access (2024).

[19] Anguiano-Gijón, Carlos A., et al. "Assessment of Petri nets Regulation Control methodologies for automation systems." Control Engineering Practice 144 (2024): 105819.

[20] Petty, Mikel D., et al. "Simulating cyberattacks with extended Petri nets." SIMULATION 100.12 (2024): 1257-1280.

[21] Yang, Yang, et al. "Research on Dynamic Data Security Protection Model Based on Petri Nets." Proceedings of the 2024 International Conference on Machine Intelligence and Digital Applications. 2024.

[22] Alisher, O., Inomjon, Y., Quvvatali, R., Sherzodjon, R., Zilolaxon, M. (2026). Development of an Algorithmic Model of Access Management Based on Phishing Detection. In: Swaroop, A., Virdee, B., Correia, S.D., Polkowski, Z. (eds) Proceedings of Data Analytics and Management. ICDAM 2025. Lecture Notes in Networks and Systems, vol 1600. Springer, Cham. https://doi.org/10.1007/978-3-032-03072-6_20

[23] Alisher, O., Inomjon, Y., Quvvatali, R., Sherzodjon, R., Zilolaxon, M. (2026). Mathematical Formalization of Detection and Prevention of Phishing URLs Based on Functioning Tables. In: Swaroop, A., Virdee, B., Correia, S., Polkowski, Z. (eds) Proceedings of Data Analytics and Management. ICDAM 2025. Lecture Notes in Networks and Systems, vol 1602. Springer, Cham. https://doi.org/10.1007/978-3-032-03558-5_11

[24] A. Kabulov, I. Yarashov and A. Otakhonov, "Algorithmic Analysis of the System Based on the Functioning Table and Information Security," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795746.

[25] Kabulov, A. V., Normatov, I. H. About problems of decoding and searching for the maximum upper zero of discrete monotone functions. Journal of Physics: Conference Series, 1260(10), 102006, 2019. doi:10.1088/1742-6596/1260/10/102006

[26] Kabulov, A.; Saymanov, I.; Babadjanov, A.; Babadzhanov, A. Algebraic Recognition Approach in IoT Ecosystem. Mathematics 2024, 12(7), 1086. https://doi.org/10.3390/math12071086

[27] Saymanov, I. (2024). Logical automatic implementation of steganographic coding algorithms. Journal of Mathematics, Mechanics and Computer Science, 121(1), 122–131. https://doi.org/10.26577/JMMCS2024121112

[28] A. Kabulov, I. Saymanov, I. Yarashov and A. Karimov, "Using Algorithmic Modeling to Control User Access Based on Functioning Table," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-5, doi: 10.1109/IEMTRONICS55184.2022.9795850.

[29] E. Navruzov and A. Kabulov, "Detection and analysis types of DDoS attack," 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2022, pp. 1-7, doi: 10.1109/IEMTRONICS55184.2022.9795729.

[30] A. Kabulov, I. Normatov, A. Seytov and A. Kudaybergenov, "Optimal Management of Water Resources in Large Main Canals with Cascade Pumping Stations," 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2020, pp. 1-4, doi: 10.1109/IEMTRONICS51293.2020.9216402.

[31] Kabulov, A. V., Normatov, I. H., Ashurov A.O. Computational methods of minimization of multiple functions. Journal of Physics: Conference Series, 1260(10), 10200, 2019. doi:10.1088/1742-6596/1260/10/102007.

[32] A. Kabulov, I. Saymanov, I. Yarashov and F. Muxammadiev, "Algorithmic method of security of the Internet of Things based on steganographic coding," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422588.

[33] Maruf Juraev, Inomjon Yarashov, Adilbay Kudaybergenov, Alimdzhan Babadzhanov and Zilolaxon Mamatova, "Research on Network Flow Based on Statistical Analysis Methods" International Journal of Advanced Computer Science and Applications(ijacsa), 16(6), 2025. http://dx.doi.org/10.14569/IJACSA.2025.0160618

[34] Alimdzhan Babadzhanov, Inomjon Yarashov, Maruf Juraev, Alisher Otakhonov, Adilbay Kudaybergenov and Rustam Utemuratov. "Mathematical Representation of Netflow Analysis Decision Making Based on Production Logic". International Journal of Advanced Computer Science and Applications (ijacsa) 16.9 (2025). http://dx.doi.org/10.14569/IJACSA.2025.0160916

[35] Yarashov, I., Kuvonchbek, R., Juraev, M., Rahmonov, F. (2026). Processing and Analysis of Network Flow Data Using Intelligent Technologies. In: Koucheryavy, Y., Aziz, A. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. ruSMART NEW2AN 2024 2024. Lecture Notes in Computer Science, vol 15555. Springer, Cham. https://doi.org/10.1007/978-3-031-95296-8_4

[36] Juraev, M., Yarashov, I., Sadulla, A., Shavkat, I., Maksad, O. (2026). Testing TCP Protocol Flags Based on the Invariance of Petri Networks. In: Swaroop, A., Virdee, B., Correia, S.D., Polkowski, Z. (eds) Proceedings of Data Analytics and Management. ICDAM 2025. Lecture Notes in Networks and Systems, vol 1600. Springer, Cham. https://doi.org/10.1007/978-3-032-03072-6_15

[37] Yarashov, I., Juraev, M., Ismatillayev, A., & Rakhimberdiev, K. (2025). Behavior Modeling in Computerized Production Systems. In Proceedings of the 8th International Conference on Future Networks & Distributed Systems (pp. 873–880). https://doi.org/10.1145/3726122.3726249

[38] Normatov, I., Yarashov, I., Otakhonov, A., & Ergashev, B. (2022, September). Construction of reliable well distribution functions based on the principle of invariance for convenient user access control. In 2022 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-5). IEEE.

[39] Toshmatov, S., Yarashov, I., Otakhonov, A., & Ismatillayev, A. (2022, September). Designing an algorithmic formalization of threat actions based on a Functioning table. In 2022 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-5). IEEE.