IRSTI 28.17.31 DOI: https://doi.org/10.26577/JMMCS2024-v124-i4-a6

I. Normatov[1*], **I. Yarashov**[1,2], **S. Toshmatov**

[1]National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan
[2]University of World Economy and Diplomacy, Tashkent, Uzbekistan
*e-mail: ibragim_normatov@mail.ru

RESEARCH AND MODELING OF AUTHENTICATION PROCESS USING FUNCTIONING TABLE

As a result of solving certain tasks, new digital data and knowledge appear, that is, systematized factual or tested messages. They are generalized as a set of laws, theories and other ideas and views. Later, this knowledge is part of the digital data needed to solve other tasks or clarify the previous one. The number of participants in the web-based cyber system has grown substantially over the last five years, making cyberspace security and Internet security more difficult for Internet users and service providers. A functioning table-based authentication modeling is proposed to protect personal and confidential information of cyber system participants and networks in cyberspace from unauthorized access and to ensure cyber security. Social engineering and low complexity password cracking has been the cause of serious research and discussion in the field of cyber security. In this research, it is highly relevant to carry out modeling and synthesis of authentication in effective data storage and network security in cyberspace. In this work, the authentication procedure, which is one of the main components of cyber security in cyberspace, is modeled on the basis of a functional table. The attributes used in the cyber system are grouped, and research, analysis and experiments are conducted with models for the grouped parts. The purpose of this study is to show that safety increases with the number of attributes and decreases with the chance of repeating the wrong sequence of symptoms.

Key words: authentication, Functioning table, username and password, fingerprint, face identification, access process.

И. Норматов[1*], И. Ярашов[1,2], Ш. Тошматов[1]

[1]Мирзо Улугбек атындағы Өзбекстан ұлттық университеті, Ташкент қ., Өзбекстан
[2]Дүниежүзілік экономика және дипломатия университеті, Ташкент қ., Өзбекстан
*e-mail: ibragim_normatov@mail.ru

Функционалдық кестенің негізінде аутентификация процесін зерттеу және модельдеу

Белгілі бір мәселелерді шешу нәтижесінде жаңа цифрлық деректер мен білімдер, яғни жүйеленген нақты немесе тексерілген хабарламалар пайда болады. Олар заңдардың, теориялардың және басқа да идеялар мен көзқарастардың жиынтығы ретінде жинақталған. Кейінірек бұл білім басқа мәселелерді шешуге немесе алдыңғысын нақтылауға қажетті цифрлық деректердің бір бөлігіне айналады. Соңғы бес жылда веб-кибержүйеге қатысушылардың саны айтарлықтай өсті, бұл интернет пайдаланушылары мен қызмет провайдерлері үшін киберкеңістік пен интернет қауіпсіздігін күрделірек етті. Функционалдық кесте негізінде аутентификацияны модельдеу кибержүйе мен киберкеңістіктегі желілерге қатысушылардың жеке және құпия ақпаратын рұқсатсыз кіруден қорғау және киберқауіпсіздікті қамтамасыз ету үшін ұсынылады. Әлеуметтік инженерия және күрделілігі төмен парольді бұзу киберқауіпсіздік саласындағы маңызды зерттеулер мен пікірталастарды тудырды. Бұл зерттеуде ол деректерді тиімді сақтауда аутентификацияны модельдеу және синтездеу және киберкеңістіктегі желі қауіпсіздігі үшін өте өзекті. Бұл жұмыста киберкеңістіктегі киберқауіпсіздіктің негізгі компоненттерінің бірі болып табылатын аутентификация процедурасы жұмыс істейтін кесте негізінде модельденген.

Кибержүйеде қолданылатын атрибуттар топтастырылып, топтастырылған бөліктердің үлгілері бойынша зерттеу, талдау және эксперименттер жүргізіледі. Бұл зерттеудің мақсаты қауіпсіздік белгілерінің саны артқан сайын артып, симптомдардың қате реттілігінің қайталану ықтималдылығымен төмендейтінін көрсету.

Түйін сөздер: аутентификация, функционалдық кесте, пайдаланушы атымен құпия сөз, саусақ ізі, бетті сәйкестендіру, кіру процесі.

И. Норматов[1*], И. Ярашов[1,2], Ш. Тошматов[1]
[1]Национальный университет Узбекистана имени Мирзо Улугбека, г. Ташкент, Узбекистан
[2]Университет мировой экономики и дипломатии, г. Ташкент, Узбекистан
[*]e-mail: ibragim_normatov@mail.ru

Исследование и моделирование процесса аутентификации на основе таблиц функционирования

В результате решения определенных задач появляются новые цифровые данные и знания, то есть систематизированные фактические или проверенные сообщения. Они обобщены как совокупность законов, теорий и других идей и взглядов. Позже эти знания входят в состав цифровых данных, необходимых для решения других задач или уточнения предыдущей.За последние пять лет число участников сетевой киберсистемы резко возросло, но кибербезопасность в киберпространстве и безопасность в Интернете становятся все более трудными для пользователей Интернета и поставщиков услуг. Моделирование аутентификации на основе Таблицы функционирования предложено для защиты личной и конфиденциальной информации участников киберсистемы и сетей в киберпространстве от несанкционированного доступа и обеспечения кибербезопасности. Социальная инженерия и взлом паролей низкой сложности стали причиной серьезных исследований и дискуссий в области кибербезопасности. В данном исследовании весьма актуально провести моделирование и синтез аутентификации в эффективном хранении данных и сетевой безопасности в киберпространстве. В данной работе процедура аутентификации, которая является одним из основных компонентов кибербезопасности в киберпространстве, моделируется на основе функционирующей таблицы. Атрибуты, используемые в киберсистеме, сгруппированы, а исследования, анализ и эксперименты проводятся с моделями сгруппированных частей. Цель данного исследования - показать, что безопасность увеличивается с увеличением количества признаков и снижается с увеличением вероятности повторения неправильной последовательности симптомов.

Ключевые слова: аутентификация, таблиц функционирования, имя пользователя и пароль, отпечаток пальца, идентификация лица, процесс доступа.

1 Introduction

With the quick improvement of arrange applications [1–4], organize security has ended up an vital issue, and verification protocols are the establishment of security in systems. Typically why appropriate provisioning of these conventions is basic. Shockingly, it is troublesome to create a strong and viable security convention for systems. Not as it were since of the characteristics of systems, but moreover since of the need of great examination procedures [5–8]. Cryptography is the technical approach used to ensure cybersecurity in a computerized world [9–12]. Mathematics used to explain cybersecurity, including confidentiality, data integrity, access management, and authentication, is known as cryptography [13–16]. The aim of privacy is to prevent the disclosure of information to anyone except those with permission. Several privacy strategies have been developed, including mathematical algorithms that render data incomprehensible.The provision of access control entails the disabling of certain clients and applications [17–19]. The process of identifying or authenticating individuals who are requesting access requires each individual to be identified. Identity-based services are referred to as authentication.This constitutes the fundamental constituent of an online safe space. With client identity knowledge, the server can make decisions about providing services and granting special rights to clients.Increasing numbers of Internet cyberspace users over the last five years have created problems for both consumers and providers of such services. Social engineering and simple password hacking lead to serious cybersecurity problems [20–22]. To ensure a high level of cybersecurity in a cyber system, it is necessary to pay attention to the complexity of passwords. Advanced cybersecurity capabilities with multi-factor authentication [23–28] can be explored, analyzed, and modeled for Internet access. The paper proposes functioning table (FT) - based authentication modeling to protect cybersecurity from unauthorized access to personal and confidential information of cyber system users. It is also proposed to model the authentication procedure based on FT to effectively ensure data security and network security during a cyber attack(Figure 1).

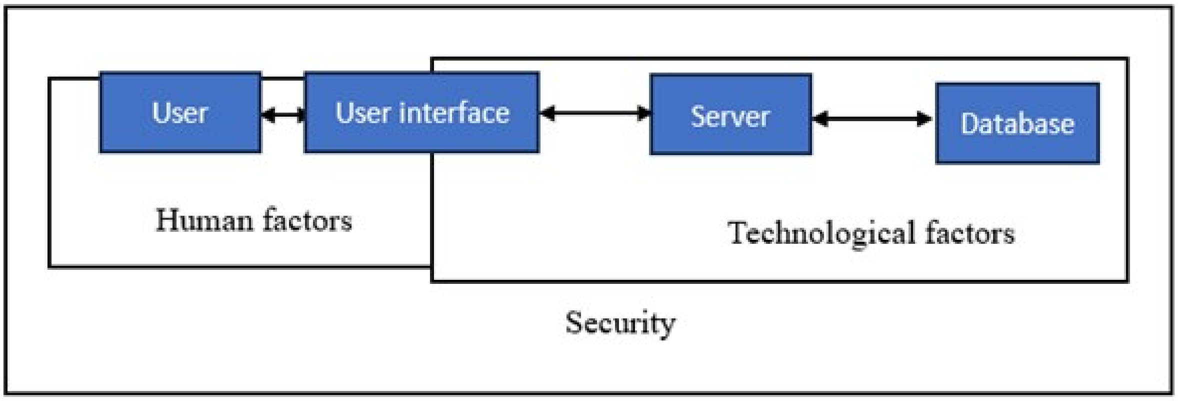

Figure 1: Username and password authentication security factors

Human factors can be classified into two categories:

Username and password type (length, randomness, used characters, etc.)

Mode in which the user protects the password (how often the user changes the password, whether the user writes down the password, etc.)

Since users are considered to be the weakest link in every security solution, it is necessary to study their behavior. Users are convinced that it is necessary to learn how to choose their passwords, because this means the security of this type of authentication.

Many authors often discuss the factors affecting password security, such as: length, randomness, and lifetime of the password. Some authors try to distinguish between "weak"and "strong"passwords, usually 0 according to the expert.

Other authors are trying to crack passwords and the results of their experiments are available as 0, 0 proof of the weakness of passwords. The authors of this article believe that some passwords need a specific number that represents the level of security. The password security feature serves a variety of purposes:

Decisions on how to perform password authentication (assessing password security as part of a risk analysis).

Surveys on long-term trends in password selection.

Password selection requests by different types of users.

To study the effect of different modes of training on password selection.

After passing into computer systems, for example in case e-business according (fig.2)

After passing into computer systems, for example in case e-business according (fig.2) Implementation of encryption algorithms and methods for inter-party communication requires a protocol.Using various primitives, including cryptographic systems, hash functions and random number generation (as opposed to complex Hash function-based protocols), one can create a protocol. To implement encryption algorithms and methods, a protocol must be established between parties involved in communication.The creation of a protocol can involve the use of cryptographic systems, hash functions, and random number generation, among other primitives. However, there are many other techniques available.

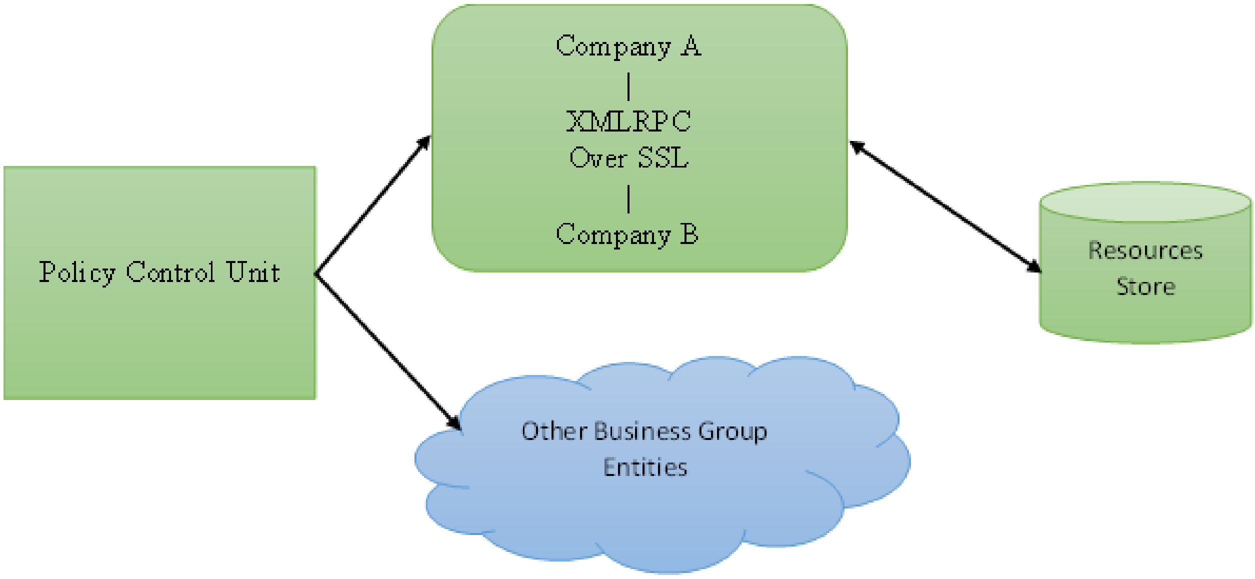

Figure 2: According to the secure communication infrastructure

The client and server must authenticate themselves before sending any messages. In the past, they used public key infrastructure (PKI) with X.509 certificates for authentication. But the first step is to use the username and password, then after the first step is successful, PKI and other methods can be used.

The opening statement details the Kerberos method and explains the reason behind its creation, given that it is susceptible to password-guessing attacks.

It then presents a brief review of related works. It then uses keyboard dynamics techniques to model username and password access to network and/or information systems from Functioning Tables. Finally, conclusions and future work are summarized.

2 RELATED WORK

Several client/server applications utilize passwords for authentication, remote access to an online database of a vendor and/or banking systems.It is common for attackers in these programs to bypass the password and send it back to the server.A system named One Time Password (OTP) System is capable of resolving this replication problem. The reason why an OTP system is preferred over a simple password system in that it generates supplementary passwords for authentication requests. This is advantageous.The password entered by the client is not transmitted across the network in a one-time password system.This approach enables OTP systems to shield clients from passive attacks. Probabilistic risk assessment (PRA) is the most powerful risk quantification method used in information security risk assessment. Key concepts such as assets, threats, vulnerabilities, exposures, probabilities and safeguards gave rise to a qualitative approach called GMITS (IT Security Assurance Management Guide) in the 1990s. A data breach encompasses any violation of confidentiality, integrity or availability:

1) Confidentiality: This ensures that information cannot be disclosed without permission or inadvertent disclosure.

2) Integrity: It is data-driven, with no inappropriate changes or corruption.

3) Availability: Users who are authorized can use applications and systems as they see fit to carry out their duties.

GMITS calculates the risk value of the information asset that is to be protected by multiplying each value of the information asset, threat, and vulnerability: $\times$ Risk value $=$ (information asset value) $\Gamma \times$ (threat value) $\Gamma \times$ (vulnerability value)

It is true that GMITS has the simplicity of assessing risk with the scores of these three factors, but GMITS cannot describe a personal data loss scenario.

The list of scenarios from the beginning of the incident to the accident is not completed. Assuming a long-term secret key is shared between the client and the Kerberos infrastructure, it is possible for kerneros to authenticate repeatedly to multiple servers. Numerous pieces have explored the security of Kerberos.It frequently highlights certain flaws in Kerberos and occasionally suggests ways to enhance it. By addressing known vulnerabilities in previous versions, this new version takes the lead in the evolution of the protocol. In recent years, the Functioning tables have been successfully used in the modeling of authentication protocols.

3 KERBEROS MESSAGE EXCHANGE

Modern computer networks rely heavily on Kerberos as the primary authentication and authorization system. All major computer operating systems now support Kerberos, which holds a unique position as enabling the use of peer-to-peer authorization and for distributed authentication.

Figure 3 illustrates the simplified Kerberos functionality.Logging in with a new login credentials is the only time that the Kerberos AS (authentication server) uses the user's username and password during the letter 1 and 2 exchange.In letters 3 and 4, the client is exchanged with the Kerberos TGS (Ticket Granting Server) when the user is authenticated to a new server.

When a user authenticates with the server, letter 5 is utilized. In the end, server response

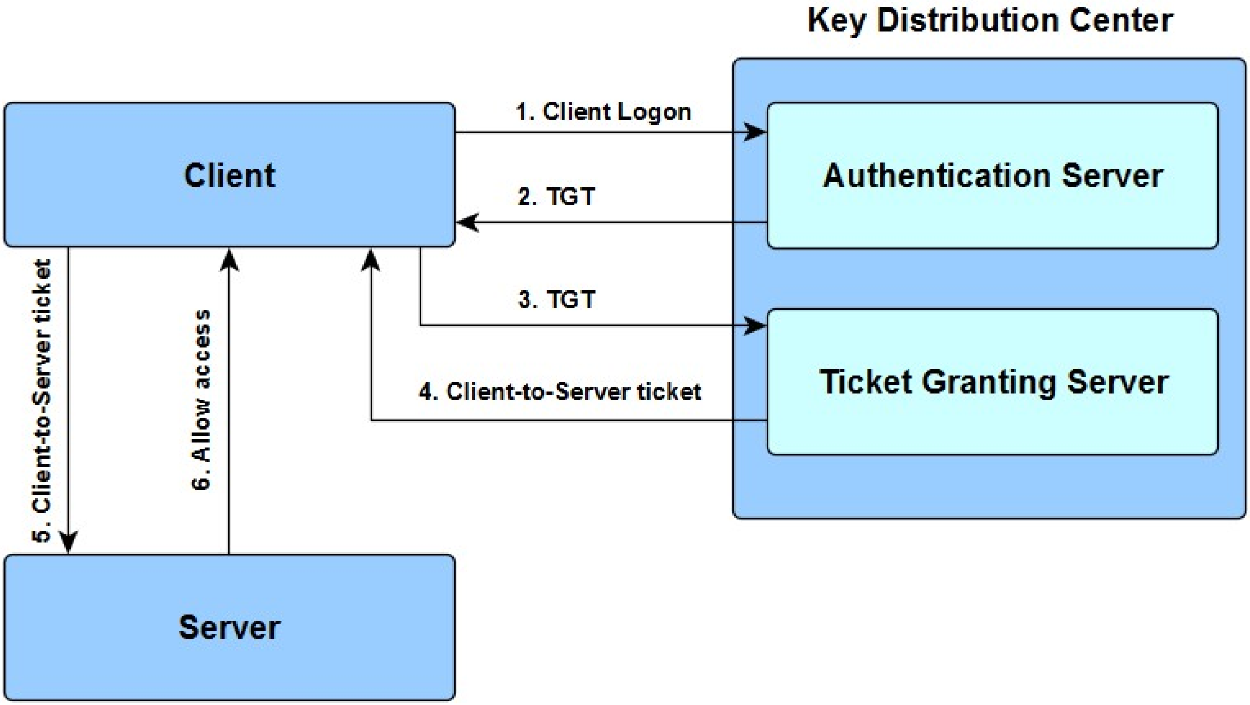

Figure 3: Overview of Kerberos operations

for mutual authentication is labelled as letter 6. Authentication of the ticket and session secret is done using user credentials linked to a particular server

The client's long-term secret key is generated using the client's username and password. The first step of the authentication process is modeled in the next part of this contribution.

4 MODELLING BY FUNCTIONING TABLES

An approach to modeling functioning tables is discussed, in which Functioning tables are described as follows: Functioning tables are a symbol for graphical and mathematical modeling, first created by Vasil Kabulov. A Functioning table consists of tables coordinates, positions, transitions, and arcs that connect them. Tables coordinates as column and row of functioning table, positions are drawn as circles, passages as rectangles, and arcs as arrows. Input arcs connect transitions, output arcs connect transitions to positions. Positions are passive components that model the state of the system. With these basic elements we can build different authentication models. The first is a model in which the username, password and fingerprint are used without the ability to correct the incorrect sequence of characters (Fig. 6). The following model allows you to correct an incorrect sequence of characters (Fig. 7). The last model is similar to the previous one, but with the ability to correct the incorrect sequence of characters in Figure 9. They may contain tokens spoken to as dark dabs. In Figure 8, the taking after demonstrate considers a combination of information confirmation and quality verification, where unique mark and confront distinguishing proof information have

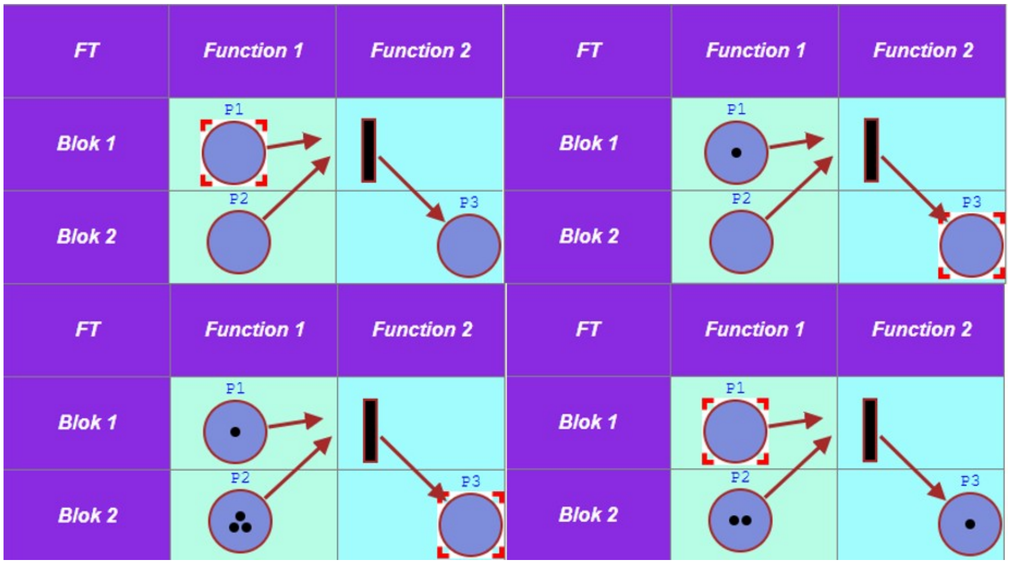

Figure 4: Functioning table elements and firing sequence modified according [33]

been chosen as the property. The current state of the Functioning table (too called checking) is given by the number of tokens in each position. A transition is an dynamic modeling movement that can happen and cause a alter of state through the unused task of tokens to positions. Transitions can as it were be made on the off chance that it is empowered, that's , there's at slightest one token at each entrance. When this happens, the switch expels a token from each input and includes a token to each yield. Due to its graphical nature, Functioning tables can be used as a visualization method like flowcharts or diagrams, but with more scope on parallelism angles. As a thorough numerical representation, formal concepts such as straight arithmetical conditions or likelihood hypothesis can be utilized to examine the behavior of the modeled framework. Many software tools have been developed to implement these techniques, a comprehensive overview can be found in the Functioning Tables Tools Database.

Functioning tables (FT) are defined as a structure $FT =< F_x; F_y; P; T; A >$, where F_x and F_y is set of tables coordinates, P means set of positions, T is set of transitions and A is $A \subseteq (PxT) \cup (TxP)$, where $(\forall t \in T)(\exists p; q \in S)(p; t); (t; q) \in A$. Graphical representation is set up by following symbols as was described above:

Coordinates of table cells of Functioning table

Positions - circles

Transitions - rectangle

Arcs - pointers between transitions and positions or places and transitions

Markers - dots

Functioning table models comprise of two parts: to begin with, the arrange structure speaking to the inactive portion of the framework, and moment, the image speaking to the common state of the structure. The dispersion of tokens between the positions of a Functioning table is called its stamping. In case one or more tokens are found within the same position, the position is said to be stamped, something else it is unmarked. The number

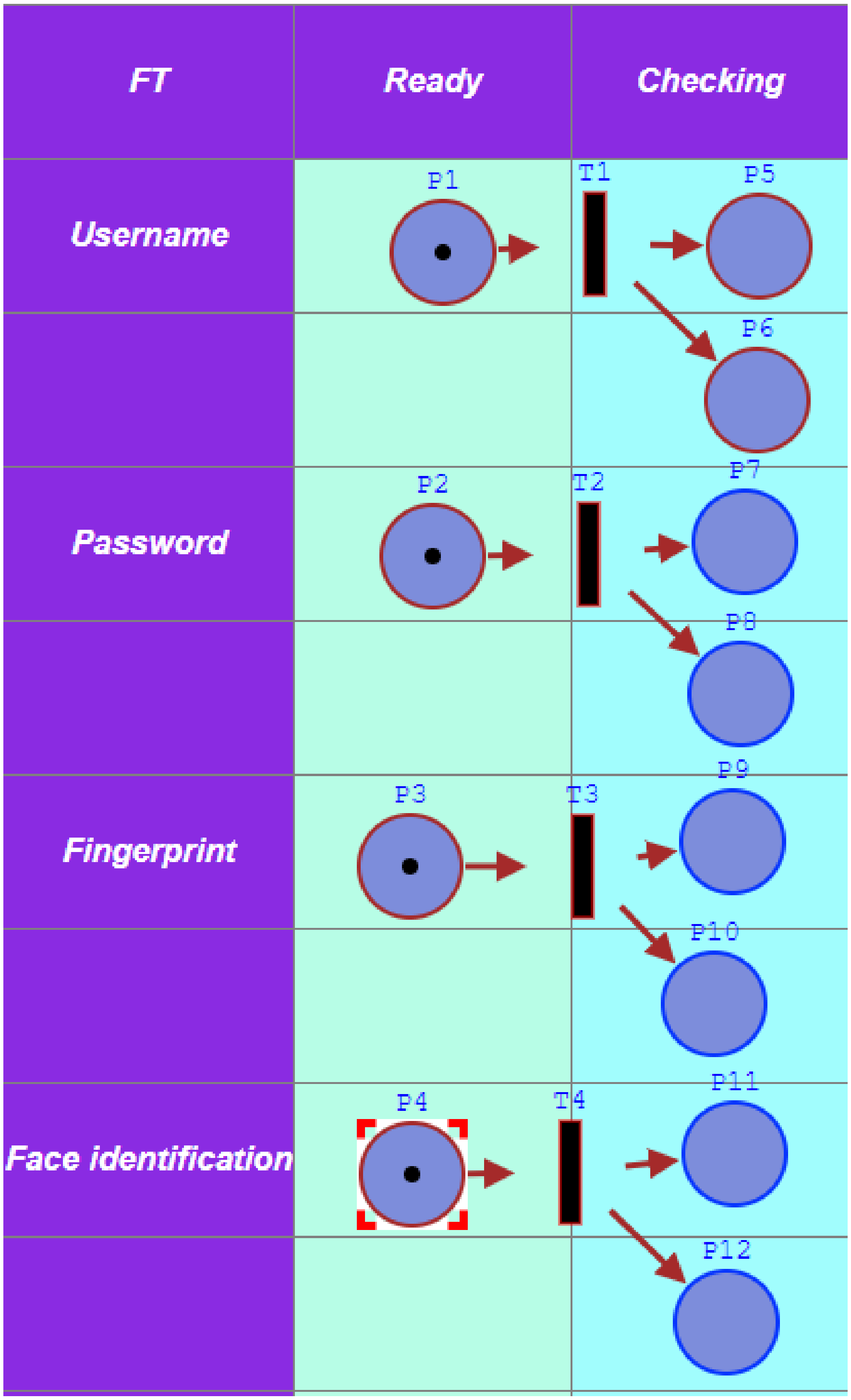

Figure 5: FT representation of username, password, fingerprint data and face identification data

of tokens in a position speaks to the nearby state of the position, whereas the token of the organize speaks to the in general state of the framework. The energetic behavior of the

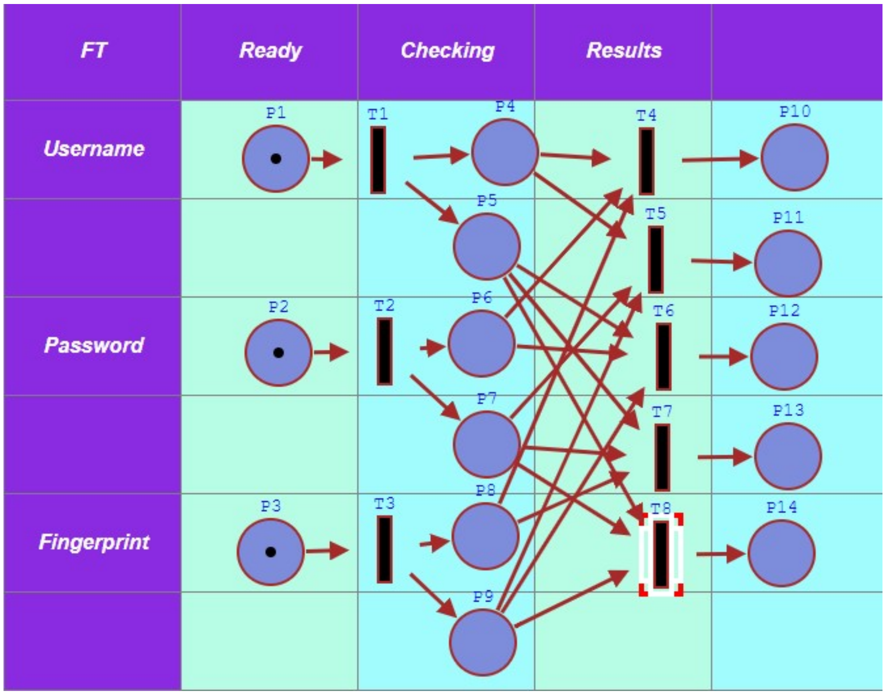

Figure 6: FT verification demonstrate utilizing username, secret word and unique finger impression information without the capacity to rectify an erroneous character arrangement

framework is at that point modeled by empowering token stream and transitions. Roughly speaking, a pass shot means that the tokens in the input positions are moved Generally talking, a pass shot implies that the tokens within the input positions are moved to the yield positions.

The transition handle incorporates the taking after steps:

A transition is said to be empowered on the off chance that each section has at slightest as numerous tokens as the weight of the circular segment interfacing them (Figure 4).

An empowered transition can be empowered by expelling a number of tokens from each input break even with to the weight of the circular segment interfacing them (Figure 4).

When a transition is activated, tokens are included to the outlets associated to the transition. The number of tokens included to each exit is break even with to the weight of the circular segment interfacing them (Fig. 4).

It ought to be famous that transitions empowered for organize 2 are never constrained to empower. In commonsense modeling, transitions can be related with outside conditions that decide whether or not they fire when turned on. In addition, in a Functioning table show with no worldly properties, terminating happens instantaneously (Fig. 4). The mechanism described above is commonly referred to as the firing rule. Numerically, the investigation of Functioning tables can be done by counting all conceivable symbols to make capability trees and/or utilizing procedures and theories in discrete science such as lattice conditions. Behavioral characteristics of Functioning tables are summarized as takes after:

1. Reachability - decides whether a framework can accomplish a certain state or show a certain utilitarian behavior. The set of reachability conceivable outcomes can be indicated

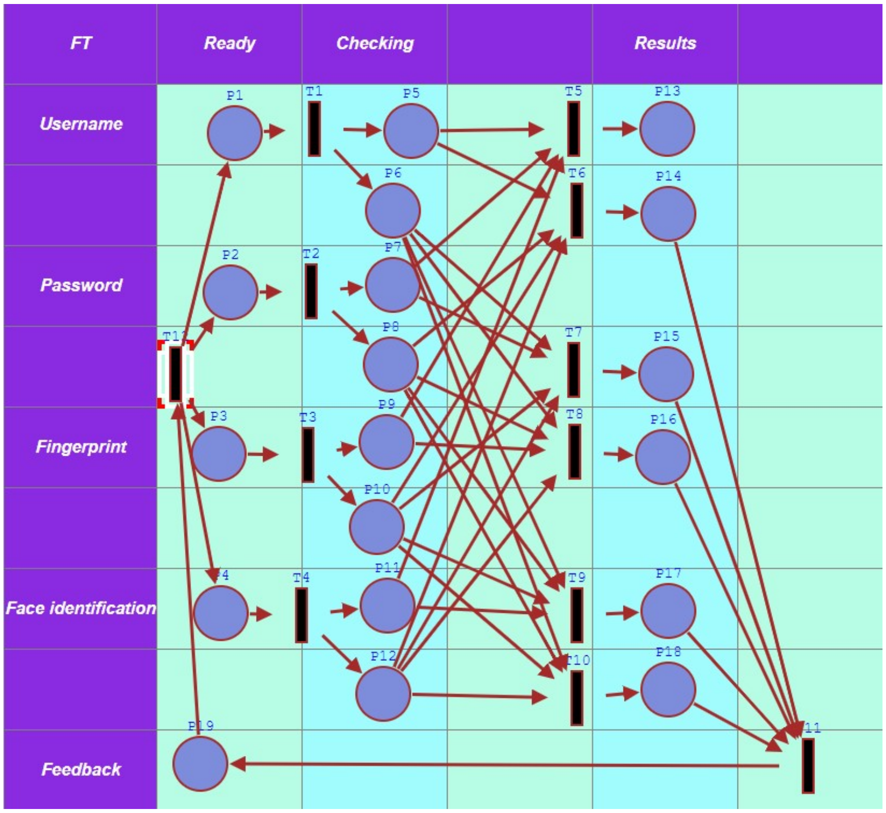

Figure 7: FT authentication model using username, password, fingerprint and face identification data with the ability to correct incorrect character sequences

by R(M0), where M0 is the beginning name.

2. Survivability - decides whether a deadlock circumstance will emerge within the framework or not.

3. Restriction and safety. A Functioning table is said to be bounded and secure unless flood conditions are identified.

4. Conservative. A Functioning table is said to be traditionalist on the off chance that the number of tokens within the show remains steady in any case of the markup it acknowledges.

5. Invertibility - a Functioning table is invertible, M_0 is reachable from M.

6. Indicates a particular stamping. This property decides whether the framework can be reinitialized or not.

In terms of modeling, Functioning tables have the taking after focal points:

Using Functioning tables to show highlights such as need connections, concurrency, dispute, and shared prohibition of a real-time framework is straightforward and clear.

Formal graphical representation gives a implies of outwardly speaking to a complex system being modeled for both modelers and clients.

From the point of see of investigation, Functioning tables have the taking after focal points:

Have a well-developed numerical base examination can be carried out to distinguish halts, floods and irreversible circumstances, etc.

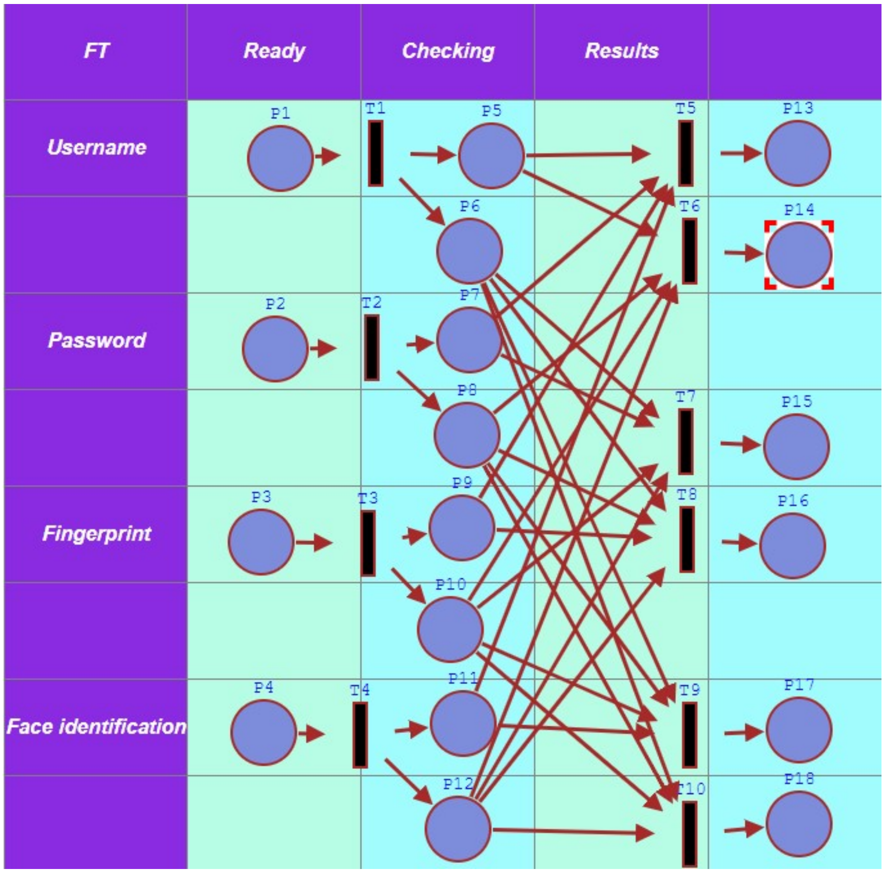

Figure 8: FT authentication model consisting of username, password, fingerprint and face identification data, without the ability to correct an incorrect character sequence

Performance assessment is conceivable through numerical investigation of the framework model.

Much research has been carried out to address the first two shortcomings in particular.

Most of them try to extend the modeling capabilities of Functioning tables by incorporating the concept of time.

It will not describe in more detail the idea and properties of the basic FT, and for a deeper understanding of this problem we recommend the basic literature [1–5], .

A basic FT representation of username, password, fingerprint data and face identification data is shown in Fig. 5.

5 Comparative analysis and experimental results

The comparison of the authentication model based on the functioning tables with other existing authentication methods is given in Table 1, which shows the advantage of the authentication model based on the FT. The effectiveness and relevance of real cybersecurity scenarios within the framework of a scientific and fundamental project are substantiated when applying an authentication model based on a functioning table in research work. The

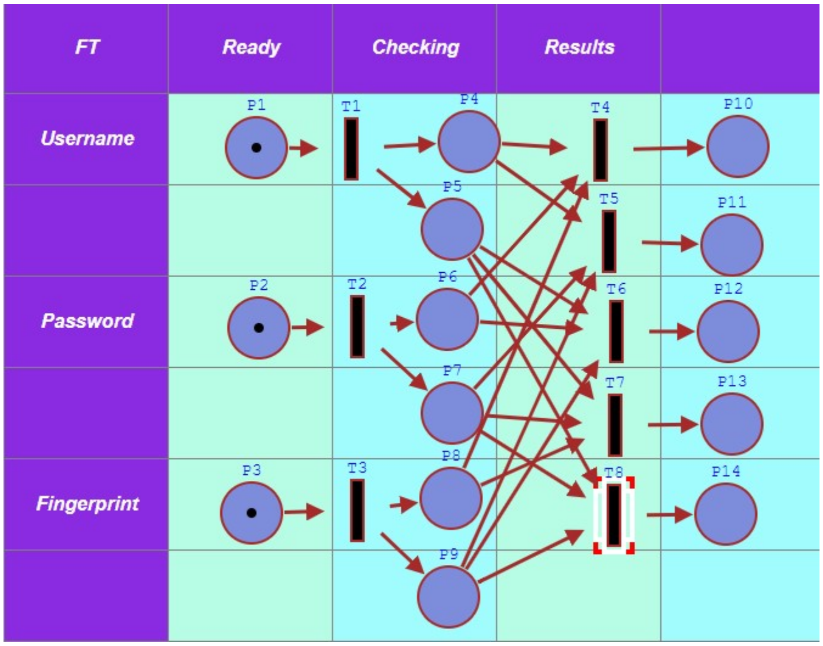

Figure 9: FT authentication model consisting of username, password, fingerprint and face identification data, with the ability to correct incorrect character sequences

Table 1: Security threats and the robustness of different authentication methods.

Threat	Password-Based Authentication	Fingerprint-Based Authentication	Face Identification Authentication	Modelled Authentication Based on Functioning Tables
Password Theft	Secure	Not Applicable	Not Applicable	Secure
Phishing Attacks	Secure	Not Applicable	Not Applicable	Secure
Password Forgery	Secure	Not Applicable	Not Applicable	Secure
Fingerprint Forgery	Not Applicable	Secure	Not Applicable	Secure
Fingerprint Reading Errors	Not Applicable	Secure	Not Applicable	Secure
Fingerprint Copying	Not Applicable	Secure	Not Applicable	Secure
Face Forgery	Not Applicable	Not Applicable	Secure	Secure
Face Recognition Errors	Not Applicable	Not Applicable	Secure	Secure
Appearance Changes	Not Applicable	Not Applicable	Secure	Secure

results of the project are presented in the form of an empirical study. An empirical test of the proposed authentication model was carried out to assess its effectiveness in various cybersecurity environments (Table 2).

Functioning table-based authentication model summarizes the advantages of the above models and provides an opportunity to structurally model and analyze their shortcomings. Therefore, it can provide relatively better solutions to researchers.

Implementation problems: practical problems in implementing the proposed model in real scenarios arise when using it in the form of a single program to organize a perfected structure. In solving this problem, it is possible to propose to divide the program into parts and use them in a mutually integrated manner.

Table 2: Access situation modeled in Fig. 8 and Fig. 9.

Username	Password	Fingerprint	Face Identification	[%] for access status in Fig. 8	[%] for access status in Fig. 9
True	True	True	True	10.7	23.1
True	True	True	False	5.7	4.5
True	True	False	True	5.3	5.0
True	True	False	False	4.7	3.3
True	False	True	True	6.6	4.4
True	False	True	False	5.5	5.3
True	False	False	True	5.3	4.2
True	False	False	False	6.2	4.9
False	True	True	True	11.7	7.2
False	True	True	False	4.6	4.5
False	True	False	True	5.2	3.9
False	True	False	False	4.9	3.8
False	False	True	True	6.7	5.4
False	False	True	False	5.4	3.1
False	False	False	True	5.2	3.6
False	False	False	False	6.3	17.8
Total Percentage of Failed Access Attempts				89.3	76.9
Total				100	100

6 Conclusion

The initial stages of modeling the authentication process using FT in the field of information security have not been implemented. This simulation method does not cover the learning needs of key dynamics. The FT modeling technique serves as a good tool for experimenting with authentication processes for access to information systems.

References

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

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

[3] Mansour A., Eddermoug N., Sadik M., Sabir E., Azmi M., Jebbar M. A Lightweight Seamless Unimodal Biometric Authentication System. *Procedia Computer Science*, (2024): 190-197.

[4] Ferdus M. Z., Monsur M. H., Akhtar M. J., Islam S. Secured Auto Encryption and Authentication Process for Cloud Computing Security. *Valley International Journal Digital Library*, (2024): 1040-1044.

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

[6] Mujinga M. Usable Security of Online Banking Authentication: An Exploratory Factor Analysis. *Journal of Information Systems and Informatics*,(2024(6(1)):409-420.

[7] Wang W., Li G., Chu Z., Li H., Faccio D. Two-Factor Authentication Approach Based on Behavior Patterns for Defeating Puppet Attacks. *IEEE Sensors Journal*,(2024).

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

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

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

[11] Xie D., Yang J., Wu B., Bian W., Chen F., Wang T. An Effectively Applicable to Resource Constrained Devices and Semi-trusted Servers Authenticated Key Agreement Scheme. *IEEE Transactions on Information Forensics and Security*,(2024).

[12] Park S., Wang X., Chen K., Lee Y. STATION: Gesture-Based Authentication for Voice Interfaces.*IEEE Internet of Things Journal*,(2024).

[13] AlQahtani A. A. S., Alshayeb T., Nabil M.,Patooghy A. Leveraging Machine Learning for Wi-Fi-based Environmental Continuous Two-Factor Authentication.*IEEE Access*,(2024).

[14] Tandon R., Verma A., Gupta P. K. D-BLAC: A dual blockchain-based decentralized architecture for authentication and communication in VANET. *Expert Systems with Applications*,(2024):237, 121461.

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

[16] Kabulov A., Baizhumanov A., Saymanov I. Synthesis of Optimal Correction Functions in the Class of Disjunctive Normal Forms. *Mathematics*, 2024, vol. 12, no. 13, 2120. doi: 10.3390/math12132120.

[17] Kabulov A., Baizhumanov A., Saymanov I., Berdimurodov M. Effective methods for solving systems of nonlinear equations of the algebra of logic based on disjunctions of complex conjunctions. *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, 2022, doi: 10.1109/ICSINTESA56431.2022.10041680.

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

[19] Kabulov A., Saymanov I., Babadjanov A., Babadzhanov A. Algebraic Recognition Approach in IoT Ecosystem. *Mathematics*, vol. 12, no.7, 1086, 2024: 1-26. https://doi.org/10.3390/math12071086.

[20] 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.

[21] 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.

[22] Ometov A., Bezzateev S., Mkitalo N., Andreev S., Mikkonen T., Koucheryavy Y. Multi-factor authentication: A survey. *Cryptography*,(2018):2(1), 1.

[23] ALSaleem B.O., Alshoshan A. I. Multi-factor authentication to systems login.*In 2021 National Computing Colleges Conference (NCCC)*,(2021, March):1-4,IEEE.

[24] Jacomme C., Kremer S. An extensive formal analysis of multi-factor authentication protocols. *ACM Transactions on Privacy and Security (TOPS)*,(2021(24(2)): 1-34.

[25] Suleski T., Ahmed M., Yang W., Wang E., A review of multi-factor authentication in the Internet of Healthcare Things.*Digital Health*,(2023(9)):20552076231177144.

[26] Babadzhanov A., Urunbaev E., Saymanov I., Problem of Synthesis of Minimal Forms of Logical Functions. *2022 International Conference on Information Science and Communications Technologies (ICISCT)*, 2022. doi: 10.1109/ICISCT55600.2022.10146903.

[27] Kabulov A., Baizhumanov A., Saymanov I., Berdimurodov M. Algorithms for Minimizing Disjunctions of Complex Conjunctions Based on First-Order Neighborhood Information for Solving Systems of Boolean Equations. *2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA)*, 2022, doi: 10.1109/ICSINTESA56431.2022.10041529.

[28] Li W., Cheng H., Wang P., Liang K. Practical threshold multi-factor authentication. *IEEE transactions on information forensics and security*,(2021(16)):3573-3588.

Information about authors:
Ibrokhimali Normatov – Doctor of Physical and Mathematical Sciences, Professor of the Faculty of Applied Mathematics and Intellectual Technologies of National University of Uzbekistan named after Mirzo Ulugbek (Tashkent, Uzbekistan, e-mail: ibragim_normatov@mail.ru);

Inomjon Yarashov – He is currently pursuing the Ph.D degree with the National University of Uzbekistan (Tashkent, Uzbekistan, e-mail: Timprivate345@gmail.com);

Shukhrat Toshmatov – Doctor of Economics, The first Vice-rector of the National University of Uzbekistan(Tashkent, Uzbekistan, e-mail: 19_sim_92@mail.ru).

Авторлар туралы мәлімет:
Иброхимали Норматов – физика -математика ғылымдарының докторы, Мирзо Улугбек атындағы Өзбекстан ұлттық университетінің қолданбалы математика және интеллектуалдық технологиялар факультетінің профессоры (Ташкент қ., Өзбекстан, e-mail: ibragim_normatov@mail.ru);

Иномжон Ярашов – Қазіргі уақытта Өзбекстан ұлттық университетінде PhD дәрежесін алуда (Ташкент қ., Өзбекстан, e-mail: Timprivate345@gmail.com);

Шухрат Тошматов – экономика ғылымдарының докторы, Өзбекстан ұлттық университетінің бірінші проректоры (Ташкент қ., Өзбекстан, e-mail: 19_sim_92@mail.ru).

Received: May 12, 2024
Accepted: December 7, 2024