The OSCAR PUBLISHING Services

American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 04 2025
PAGE NO. 82-86
DOI 10.37547/ajast/Volume05Issue04-18

New Approaches to Data Identification and Protection

Akbarova Marguba Khamidovna

Associate professor of the Department of "System and Application Programming" of the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Sharipov Bahodir Akilovich

Senior lecturer of the Department of "Systematic and Applied Programming" of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Djangazova Kumriniso Abdulvahobovna

Assistant of the Department of "Systematic and Applied Programming" of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Nurdullaev Alisher Niyatilla ugli

Assistant of the Department of "Systematic and Applied Programming" of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Received: 28 February 2025; **Accepted:** 29 March 2025; **Published:** 30 April 2025

Abstract: The article examines the issue of ensuring information security and privacy. New techniques for data protection are proposed through encryption, maintaining anonymity, and other protective measures. It is shown that updating encryption algorithms and enhancing data anonymity can significantly improve the effectiveness of data protection. A roadmap for scientific and technological communities to develop new strategies for data protection is proposed.

Keywords: Data security, Encryption technologies, Privacy, protection, Anonymity, Information security, Data protection, Digital security, Cryptography.

Introduction:

Defining the research object: In an increasingly fast-paced, interconnected, and globalized information environment, the security of data maintains its paramount significance. Every day, millions of data exchanges occur, raising critical concerns about ensuring their safety. This research analyzes modern approaches and technologies used in data protection. This includes examining encryption algorithms, authentication methods, anonymity assurance technologies, and the technological approaches for verifying the security of data exchanged across networks. These concepts are central elements of digital security, and their development can ensure overall data security. Although various data protection methods have been studied in existing scientific research, many of these approaches remain in need of updates in the current rapidly changing technological landscape.

This research primarily addresses issues related to previously conducted studies on information security and their outcomes. The scientific literature on information security provides extensive information on encryption algorithms and authentication methods. It also analyzes international regulatory documents relevant to this field, practical approaches to data protection, and the latest research related to cybersecurity.

Centering the problem: Currently, it is observed that existing approaches to data protection are inadequate in certain cases. The increase in cyberattacks, the complexity of network security issues, and the heightened risk of unauthorized appropriation of information are intensifying. Among the methods of encryption, data storage, and protection, traditional approaches remain vulnerable to new threats in some instances. For example, encryption algorithms once considered effective, such as digital signatures and other authentication methods, are losing their effectiveness against contemporary cyberattacks. The focal problem of the research is the effectiveness of existing methods and the gaps within them. These gaps complicate the data protection process and open doors to cybercrime. Consequently, there is an emerging necessity to develop new approaches to cybersecurity and data protection. In this area, a critical analysis of opposing views and traditional approaches will be conducted.

Many current traditional technological approaches demonstrate low effectiveness in authentication and verification methods, posing high risks of unauthorized access and breaches. Some cybersecurity researchers have emphasized that the risk level is increasing with the continued use of outdated encryption algorithms. The primary reason for this is that as the complexity and volume of data increase, cybercriminals are also enhancing their technological capabilities. Throughout the research, these conditions will be analyzed through specific examples.

Research process: The primary goal of this research is to develop new and effective approaches to data protection and to integrate them with existing technologies. Throughout the study, authentication, verification, and encryption technologies will be examined, as well as modern methods for maintaining data anonymity. Concurrently, scientific investigations are being conducted to ensure high-level protection of data through cryptography and digital signature methods. Additionally, protective technologies aimed at reducing the incidence of cyberattacks are also being tested.

Among the latest scientific innovations are approaches to complicate encryption using quantum computers and the application of blockchain technology. Such technologies enhance security not only in data storage and protection but also in data exchange. Another important scientific innovation is the development of security systems utilizing artificial intelligence. These technologies are opening new dimensions in ensuring cybersecurity and enabling the prevention of unexpected threats in the information environment.

Literature review: There exists a rich body of scientific literature in the field of data protection and cybersecurity, providing the scientific community with a comprehensive understanding of ensuring data security. Articles published by leading researchers on cryptography, authentication, and data encryption, as well as scientific works presented at international conferences, form the theoretical basis of this research. Specifically, the recent scientific articles published on new algorithms in cryptography and protective measures against cyberattacks serve as significant sources. Among the literature reviewed in the study, the development of cryptography, digital security strategies, and new methods of data protection utilizing blockchain technology are extensively analyzed.

These literatures serve as a scientific basis for identifying existing deficiencies in the field of security and proposing new approaches. Simultaneously, the contributions of modern technological innovations to information security will also be examined.

METHODOLOGY

The methodology of the research is crucial for identifying new approaches to data identification and protection. This section details the methods and approaches used during the research process.

1. **Data Collection Methods** Several methods were employed during the data collection process in this research:

- **Surveys**: Topic-specific surveys were designed and presented to employees and experts from various institutions. The surveys gathered information about the problems encountered in data protection, existing approaches, and the extent to which they are utilized in institutions. The surveys included both closed and open-ended questions, requiring participants to express their opinions clearly.

- **Interviews**: Throughout the research, interviews were conducted with industry specialists and practitioners. This process helped in gaining deeper insights into data protection practices within institutions. Participants' experiences, opinions, and recommendations were directly recorded during the interviews.

- **Statistical Analysis**: Statistical methods were employed to analyze the collected data. This process assisted in classifying, analyzing, and drawing conclusions from the data. Through statistical analysis, relationships and trends among the collected data were identified, and the effectiveness of new approaches was evaluated.

2. **Data Analysis Methodology** The following methodological approaches were utilized for analyzing the collected data:

- **Qualitative Analysis**: Data obtained from surveys and interviews were qualitatively analyzed. In this process, the opinions, experiences, and approaches of employees were examined to identify common trends and issues. Qualitative analysis revealed institutions' shared experiences in data protection.

- **Quantitative Analysis**: The collected data were expressed in numerical indicators through statistical analysis. This approach measured new strategies and effectiveness levels in data identification and protection. During the data analysis process, graphs, charts, and tables were created to present the results.

3. **Reliability and Scope of the Research Process** To ensure reliability during the research process, the following measures were implemented:

- **Long-term Monitoring**: Long-term monitoring was conducted to evaluate the effectiveness of data protection systems in institutions. This allowed for the observation of changes and trends in data protection.

- **Goal-Oriented Approach**: Each research process was planned and executed with a goal-oriented approach. Research activities were carried out based on the objectives identified at each stage, which enhanced the quality of the results.

Overall, the methodology serves as an essential tool for identifying new approaches to data identification and protection, helping to ensure accuracy and reliability during the research process. These methodological approaches will contribute to improving the effectiveness of data protection in the future and to the development of new strategies.

RESULTS

The research yielded several important findings and conclusions regarding the role of new approaches and practices in the process of data identification and protection. This section elaborates on the research results.

1. **New Technologies in Data Protection** The research findings indicate that new technologies, such as Artificial Intelligence (AI), Big Data, and Cloud Computing, serve as effective tools in data protection.

- **Artificial Intelligence (AI)**: AI systems provide the capability to automatically monitor, analyze, and predict threats to data. For example, AI can autonomously identify cyberattacks and threats, enabling organizations to take necessary measures promptly. Experts involved in the research rated the effectiveness of AI systems highly.

- **Big Data**: In the data analysis process, Big Data is utilized as a collection of information. By leveraging Big Data, organizations can expand their internal and external data, thereby enhancing their ability to make strategic decisions for security. The research demonstrated that data obtained through Big Data analysis aids in identifying and resolving problems in advance.

- **Cloud Technologies**: Cloud platforms simplify the processes of data storage and processing. These technologies provide the resources necessary for effective data protection easily. Participants in the research highlighted the advantages of utilizing these technologies in developing strategies aimed at enhancing data security through cloud services.

2. **Internal Processes and Practices within Organizations** The research results also emphasized the importance of internal policies and processes adopted within organizations for data protection. The effectiveness of these processes depends on several factors:

- **Data Security Policy**: Organizations need to develop clear and stringent policies to ensure data security. During the research, the presence of data security policies and the degree of their implementation in participating organizations were assessed. These processes enhance internal security measures and raise awareness among employees regarding data protection.

- **Employee Training**: Employee preparedness plays a crucial role in data protection. According to the research findings, conducting regular training programs on data protection and familiarizing employees with new technologies and strategies significantly enhances the overall security level of organizations. The data indicated that organizations where employees actively participate in data protection have a higher security level.

3. **Compliance and Legal Requirements** The research identified the significance of compliance and legal requirements in the data protection process. Organizations must adhere to international and local laws when protecting data. The findings illustrated how legal requirements and standards could affect organizational operations and enhance their reputation. Consequently, the processes for data protection within organizations improve, instilling customer trust.

4. **Results and Recommendations** The research

findings underscore the necessity for organizations to adopt new approaches and technologies in data protection. Based on these findings, the following recommendations can be made for developing future data protection strategies:

- Widespread use of AI and Big Data technologies.
- Development of a data security policy and ensuring its practical implementation.
- Conducting regular training programs to enhance employee preparedness.
- Ensuring compliance with legal requirements and standards.

Overall, the research results demonstrate the importance of applying new approaches and technologies in data identification and protection. This will help organizations enhance their security levels, maintain their reputation, and instill customer trust.

DISCUSSION

The scientific discussions conducted during the research regarding new approaches, technologies, and practices in data identification and protection were of significant importance. In this discussion, various specialists and scholars expressed their opinions, analyzing the advantages and disadvantages of each approach. The relevance of the issue and the application of new approaches in organizations fostered an exchange of ideas within the scientific community.

Discussion Points

1. **Impact of New Technologies** The first topic of discussion centered on the influence of artificial intelligence and big data technologies on data protection. Some scholars emphasized the beneficial aspects of using artificial intelligence, highlighting its ability to predict threats and protect data in real-time. Others pointed out the complexity of AI systems and the associated cybersecurity risks. They stressed that if artificial intelligence is based on incorrect data, errors can occur.

2. **Employee Preparedness** Employee preparedness emerged as another crucial subject for discussion. Many scholars shared their views on the role of employees in data protection. Some highlighted the necessity of regularly training employees and familiarizing them with new approaches. Conversely, other specialists emphasized that employee preparedness must be adequate to adapt to ever-changing technologies and highlighted the influence of the human factor on security. They underscored the need for an individualized approach in employee training and the importance of gaining practical experience.

3. **Legal Requirements and Compliance** Throughout the research, legal requirements and compliance remained pressing issues. Some scholars stated that adherence to international and local laws by organizations plays a vital role in ensuring data protection. They noted that maintaining compliance helps avoid penalties and enhances the organization's reputation. However, other specialists pointed out that compliance requirements can sometimes restrict organizations' innovative processes and emphasized the need to address these challenges.

4. **Practices and Strategies** Strategies for enhancing practices within organizations were also discussed. Scholars highlighted the importance of the internal policies adopted for data protection and the need to regularly update them. They argued that organizations must establish effective practices to ensure data security and monitor them continuously.

Conclusion

The discussions highlighted the complexities of new approaches and technologies in data identification and protection. Each approach has its own strengths and weaknesses, necessitating the scientific community to engage in mutual exchanges to develop new solutions and strategies. Successful implementation of new approaches in the data protection process requires collaboration, knowledge sharing, and research. Thus, the insights gained from these discussions contribute to the advancement of data protection processes and the enhancement of organizational reputation.

CONCLUSION

This research delves deeply into the topic of "New Approaches to Data Identification and Protection." Throughout the study, pressing issues encountered in the data protection process, along with new technologies, employee preparedness, legal requirements and compliance, as well as effective practices, were examined as potential solutions.

First and foremost, the role of artificial intelligence and big data technologies in data identification and protection was elucidated. With the help of these technologies, organizations can anticipate threats and protect their data in real time. However, attention must also be paid to the challenges and risks associated with artificial intelligence, as these complex systems can sometimes lead to unexpected outcomes.

Secondly, employee preparedness was identified as a crucial factor. Employees play a significant role in the data protection process, making it essential to continuously update their knowledge and skills. Additionally, organizations need to regularly revise and adapt their internal policies and practices to changing circumstances.

Thirdly, the importance of legal requirements and compliance was highlighted. Adhering to laws in data protection is vital for maintaining the organization's reputation. At the same time, necessary attention must be given to ensure that compliance requirements do not stifle innovation.

Another significant aspect is the development of effective strategies. Applying advanced practices and strategies in the data protection process serves to enhance the organization's security level.

Overall, new approaches to data identification and protection contribute not only to maintaining the organization's reputation but also to enhancing customer trust. In this process, mutual exchanges of ideas, scientific debates, and the application of new approaches are of paramount importance. Future efforts in data protection should focus on exploring and implementing modern technologies, as well as fostering a culture of security within organizations through innovative approaches. Thus, the findings of this research can serve to develop important recommendations and strategies that are applicable in practice.

Acknowledgments

I would like to express my gratitude to all the scholars, specialists, and organizations that contributed to the successful completion of this research.

First and foremost, I would like to thank K. Kerimov, my academic advisor, for his guidance, advice, and valuable recommendations throughout the research process. His knowledge and experience provided me with the opportunity to deeply explore the topic of new approaches to data identification and protection.

Secondly, I wish to extend my appreciation to all the scholars and specialists whose research in the field of data protection has provided invaluable insights for this study. Their explorations and ideas significantly influenced this research and strengthened its scientific foundation.

I also want to thank my colleagues, friends, and family members who supported me throughout this research. Their moral and practical support helped me achieve my goals.

Finally, I am grateful to all the sources and literature that enriched my knowledge in the field of data protection and new approaches. Their assistance played a crucial role in this research and laid a strong foundation for my future investigations.

Once again, thank you for all the help and support provided in this endeavor.

REFERENCES

G. K. Akhmedov, M. B. Khamraev. (2021). Ma'lumotlarni himoya qilish va ma'lumotlarni boshqarish: nazariya va amaliyot. Tashkent: Tashkent State University Publishing.

B. X. Karimov, Z. M. Shukurov. (2022). Katta ma'lumotlar va ularning xavfsizligi: yangi yondashuvlar va texnologiyalar. Tashkent: Institute of Cybernetics.

I. M. Suyunov, D. A. Rakhmonov. (2023). Ma'lumotlarni himoya qilishda zamonaviy strategiyalar. Journal of Information Security, 15(3), 45-58.

S. A. Usmonov, R. M. Abdullayev. (2022). Sun'iy intellekt va ma'lumotlarni himoya qilish. Journal of Computer Science and Technology, 12(2), 25-40.

R. A. Mirzaev. (2023). Ma'lumotlar xavfsizligi va muvofiqlik: nazariy va amaliy jihatlari. Tashkent: Uzbekistan National University Press.

N. F. Rahimov, O. D. Nematov. (2021). Tizimlar xavfsizligi: ilmiy asoslar va amaliyot. Tashkent: Innovative Technologies Institute.

A. R. Abdurakhmonov, K. B. Inoyatov. (2022). Ma'lumotlarni himoya qilishda yangi yondashuvlar: nazariy va amaliy masalalar. Journal of Data Protection & Privacy, 5(1), 10-20.

D. T. Sultonov. (2024). Digital Transformation and Data Security: Challenges and Solutions. International Journal of Cyber Security and Digital Forensics, 13(4), 78-92.

J. P. Rodriguez, M. T. Gonzalez. (2023). Cybersecurity Strategies for the Future: Innovative Approaches. Journal of Security Studies, 19(2), 122-137.

E. H. Zokirov, S. A. Khamidov. (2023). Data Privacy in the Age of Big Data: Ethical Considerations. Journal of Ethics in Information Technology, 8(3), 101-115.