Baku State University Journal of Mathematics & Computer Sciences ***2024, v. 1 (4), p. 29-38***

journal homepage: http://bsuj.bsu.edu.az/en

ENSURİNG SECURİTY AND USER ACCESSİBİLİTY İN İNFORMATİON SYSTEMS THROUGH CRYPTOGRAPHİC METHODS

Intigam A. Maharramov

Baku State University

Received 21 semtember 2024; accepted 25 october2024

https://doi.org/10.30546/209501.101.2025.2.1.07

Abstract

This paper analyzes the developments in managing user accessibility in modern information systems and explores new security approaches. The application of artificial intelligence (AI) and machine learning (ML) technologies enables the real-time analysis of user behavior, ensuring the dynamic and effective implementation of security protocols. Quantum cryptography, by overcoming the potential vulnerabilities of traditional encryption methods due to quantum computers, elevates the security of data to a higher level.

Keywords: user accessibility, security policy, cryptographic protocols, accessibility management, Zero Trust architecture, Artificial Intelligence, Quantum cryptography

Mathematics Subject Classification *(2020): 34A30, 34B09, 34B15, 34C23, , 47J10, 47J15*

1. Introduction

Information Systems (IS) in the modern era are complex structures that encompass vast amounts of data collected, processed, stored, made ready for dissemination, and presented to users. They not only collect and store data but also utilize various tools and technologies to analyze, process, share, and enable

users to make informed decisions. Information systems are also equipped with methods and security policies (measures) to ensure and protect **user accessibility (Access Control)**. An information system's security policy is the general configuration of standards, strategies, and technologies applied by organizations and governments to protect information systems. In today's environment, where threats like cyberattacks, data theft, data distortion, and service disruptions are on the rise, the proper formulation of this policy is crucial [3].

In information systems, user accessibility (or user permissions) refers to the process of identifying and managing users who have the right to access and use data and resources within an information system. In other words, it is a security mechanism that determines which data, functions, or resources users can access and the level of authority they possess [11].

Access issues in information systems mainly arise from the following problems:

Security vulnerabilities: Weak encryption and poor permission management can lead to unauthorized access to the system by users.

System failures: Malfunctions or failures in hardware or software may render services inaccessible.

Attacks: Types of attacks on computer networks and online services can compromise system accessibility and make services unavailable to users.

Managing user accessibility is one of the key mechanisms aimed at protecting the confidentiality, integrity, and availability of a system. In other words, only those with appropriate authorization can access specific data and services. This is a crucial mechanism for safeguarding the confidentiality, integrity, and availability of data in accordance with the organization's security policy [5]. The objectives of managing user accessibility are as follows:

1. Security: Ensuring that users can only access the data and resources they are authorized to, thus maintaining the system’s security.

2. Confidentiality: Ensuring that data is only accessible to designated users, thereby protecting personal and sensitive information.

3. Defining user rights: Determining what operations each user is allowed to perform, such as granting permissions for reading, writing, or deleting data.

4. Reporting and auditing: Keeping logs to monitor and track user activities within the system (the process of recording and monitoring activities, operations,

and events within a system or organization. These logs track who performed an operation, when, and how), which helps ensure security.

The model for managing inputs plays a central role in the formal development of an information system. The model used for security purposes, characterized by abstraction, simplicity, and adequacy, determines the flow of information entering the system and governs the rules for managing access to information. When managing user accessibility, the following models are typically used:

Role-Based Access Control (RBAC): In this approach, users are assigned specific roles (e.g., admin, user, manager), and each role is granted access rights to specific resources and operations. Access to users is controlled via these roles.

Attribute-Based Access Control (ABAC): In this model, access is based on the attributes of the user (e.g., working hours, position, or location). User rights can be defined dynamically in this approach.

User-Based Access Control (UBAC): Each user individually determines their permissions. In this model, access rights for each user are based on their unique requirements.

2. Modern Cryptography

Cryptographic-based protocols are also used to ensure accessibility in information systems. These protocols aim to ensure user identification and data security while properly managing access rights [13].

SSL/TLS (Secure Sockets Layer/Transport Layer Security) protocols are widely used for encrypting data and securely transmitting information over the internet. These protocols also ensure the authentication of user identity. SSL/TLS is primarily used to establish secure connections between web servers and browsers. When a TLS connection is established, the server's identity is verified via the server's certificate. Users trust this certificate and accept that the connection is secure. This protocol ensures the encryption of data so that it cannot be read by third parties. TLS also preserves the integrity of data and ensures that information remains unaltered during transmission.

The **Kerberos authentication protocol** is used to reliably authenticate users and services over a network. This protocol primarily uses symmetric encryption algorithms and operates with a trusted identification method. Kerberos provides

the user with a "ticket" to gain access. This ticket ensures a valid connection between the user and the service and enables the establishment of a secure connection over the network. Kerberos secures the connection between users and services with encrypted tickets and time-based restrictions.

OAuth 2.0 (Open Authorization) is a widely used protocol for authenticating user identities and managing access to resources they own. OAuth 2.0 is used to secure APIs (Application Programming Interfaces, which enable interaction between different programs or systems) and regulate the access of various applications to user data. This protocol is mainly used to grant access to user data via third-party applications. OAuth 2.0 grants users limited rights (e.g., read-only access) and allows them to access only the resources that have been specifically granted.

OpenID Connect is a protocol built on top of OAuth 2.0 that provides a more reliable method for user authentication. It is used primarily to manage user authentication for repeated logins. OpenID Connect ensures the secure transmission of data through the JWT (JSON Web Token) issued to the user, enabling both authentication and API access.

SAML (Security Assertion Markup Language) protocol is primarily used for transmitting user identity between web applications and services. This protocol is widely utilized in single sign-on (SSO) applications. SAML provides centralized authentication, allowing a user to log in once and access multiple services.

FIDO (Fast Identity Online) protocol offers passwordless authentication systems. This protocol uses biometric data (such as fingerprints, facial recognition) or physical security keys (e.g., USB devices) to ensure secure and convenient access. FIDO enables users to log in without using a password.

Multi-Factor Authentication (MFA) is an approach that requires multiple authentication methods to confirm a user's identity. MFA prevents reliance on a single factor (e.g., a password) and enhances security levels. MFA requires users to authenticate with at least two factors (password, biometric data, security tokens).

X.509 Certificates are used to establish a trusted connection between users or services. These certificates use asymmetric encryption methods to ensure the security of the connection. X.509 certificates provide unique identifiers to users or

servers, enabling authentication. They ensure the encryption of data or confirm data integrity during transmission using digital signatures.

In modern information systems, managing user access requires more complex and secure approaches. The development of technology, the rise of hybrid work environments, the use of cloud technologies, the proliferation of data, and increasing cybersecurity risks require more sophisticated and flexible access management. This extends beyond just technical aspects and encompasses legal, organizational, and social considerations. Access management is crucial for regulating, monitoring, and controlling user access to systems and resources. This issue holds significant importance for both information systems and organizational security policies in both theoretical and practical contexts.

In modern security, let us review some of the most relevant theoretical approaches to access management [4]:

One of the most current concepts in modern security approaches is the **Zero Trust Architecture**. According to the Zero Trust model, no user, device, or network is ever considered fully trustworthy. This approach is based on the following principles [8]:

User identity verification at every level: Each user and device is re-verified every time an access attempt is made.

Access is granted with the least privileges (Principle of Least Privilege): Each user is only granted access to the minimal resources necessary to perform their tasks. Even internal users can only access resources for specific needs.

Compatibility with distributed environments: This approach ensures structured security in both local and cloud-based networks, such as through VPNs, multi-factor authentication (MFA), encryption, etc.

The Zero Trust Architecture offers a more flexible and secure model for organizations. This approach allows for deeper analysis of user access, granting minimal rights to users for only the required resources.

Discretionary Access Control (DAC) provides a less rigid and more user-centered approach to managing user access. In this model, resource owners (e.g., file or system administrators) define who can access specific resources and with what rights. Key features of this approach include:

Authority of the resource owner: The user managing the resources (e.g., file owner) privately determines who can access the resource and with what rights.

Flexibility: Each user can assign access rights to resources based on their preferences.

Access permission assignment: Users determine who can access their resources and what rights they have.

The DAC model is more commonly used in smaller systems or simpler setups, as it is based on user ownership and has less complexity.

Traditional authorization models limit access to a user based on a one-time registration. However, modern systems offer **dynamic authorization**, which adjusts permissions based on user activities and context. Dynamic authorization presents users with various permissions based on:

Behavioral Access Control: This approach monitors user activities and dynamically alters access rights when suspicious behavior is detected.

Time and Location-Based Access Control: The user's identity, geographical location, and the time of access determine their rights. For example, users accessing the system outside of working hours or from specific locations may have limited access.

Role-Based Access Control (RBAC) and **Attribute-Based Access Control (ABAC)** are also widely used access control models:

RBAC: This model manages access by assigning roles to users within an organization. Each role is associated with specific resource and operation access rights. For instance, a "Manager" role may only have access to certain information.

ABAC: A more flexible and modern approach, ABAC grants access based on user attributes (e.g., job position, location, time). Access rights are determined by a broader set of conditions, not just roles, providing a dynamic and context-based solution [9].

Audit logs and tracking user activities are crucial for modern systems. Activities of users are constantly monitored, and all operations are recorded. These logs are used for the following purposes:

Detection of security incidents: Monitoring suspicious activities and abnormal behaviors helps identify security breaches or attacks at an early stage.

Compliance and conformance: Audits related to data usage and access ensure compliance with legal and industry requirements.

Single Sign-On (SSO) technology allows users to access multiple systems and services after a single login, without needing to re-enter their credentials for each additional resource. While this approach provides greater convenience, it must be properly configured to mitigate security threats. The Single Sign-On concept ensures that users and devices only access systems that are trusted and well-secured.

These approaches not only ensure that only users with the appropriate rights and permissions can access systems, but also continuously monitor and analyze the system. In this way, security risks are minimized, and a more secure environment is created.

The management of user access in information systems is implemented not only through theoretical approaches but also through practical approaches. Practical approaches involve strategies and tools used to ensure security and restrict access to authorized individuals. The most relevant practical approaches include [12]:

1. Least Privilege Principle (PoLP) – This principle grants users only the minimum rights necessary for their work. This approach is crucial for security because granting additional rights increases the risks of exploitation or mismanagement.

Practical application:

User rights adjustment: Each user is granted access rights only to resources relevant to their role. For example, a data analyst might only have read access, with no rights to write or delete.

Role assignment: System access rights are defined based on user roles. For example, administrator rights are only given to those performing core management tasks, while other users may only have user or guest roles.

2. Access Control Lists (ACLs) – Access Control Lists are simple lists that grant or deny users or devices access to resources. Each resource has a designated list, specifying who can access it, when, and how.

Practical application:

ACLs in file systems: Lists that define who can access each file or directory.

ACLs in network devices: ACLs used on routers or firewalls define when and which devices can accept network traffic.

3. Identity and Access Management (IAM) – IAM systems manage user identities, assign appropriate access rights, and ensure availability. IAM systems enable centralized management of user rights within modern companies.

Practical application:

Centralized authentication for multiple services: For example, a company may require a single authentication (Single Sign-On, SSO) for users to access various systems such as email, internal applications, and network resources.

Monitoring and reporting: IAM systems track user activities and help analyze any suspicious actions.

The centralized IAM approach consolidates user data and regulates their rights, controlling access to resources.

4. Time-based Access Control – Time-based access control systems allow users to access resources only within specific time periods. This approach is mainly used for security purposes or to limit access according to working hours.

Practical application:

Access hours: Users are allowed to access resources only during working hours, for example, from 9 AM to 6 PM.

Time restrictions: Users or guests are granted time-limited access based on specific needs.

This approach is also useful for restricting network access at non-designated times and monitoring suspicious activity.

In recent years, the development of various technologies has introduced new approaches to access and security management. Among these technologies and trends, the following stand out as the most notable [2]:

Artificial Intelligence (AI) and Machine Learning (ML): These technologies are applied to detect cyberattacks in advance, identify unusual user behaviors, and predict access threats. AI can detect security gaps by monitoring anomalies in real-time. ML, a subfield of AI, enables machines to learn from data and improve performance based on experience. ML allows computers to analyze data, identify patterns, and make predictions and decisions based on experience [6].

Post-Quantum Cryptography (PQC): Following the development of quantum computers, PQC is a field of cryptography focused on overcoming the weaknesses of classical encryption algorithms and protocols. Quantum computers, with their immense computational power, can crack these algorithms faster and more

efficiently. For instance, widely-used encryption and signature algorithms such as RSA and ECDSA can be easily broken using quantum computers [4].

Blockchain Technology: A modern digital technology used for securely, transparently, and immutably storing and transferring data. Blockchain organizes data into "blocks" which are cryptographically linked to each other, creating a "chain of blocks." This structure prevents data modification and manipulation, ensuring its integrity and security [10].

The security of information systems has become more challenging and multifaceted with the advancement of the latest technologies and user behaviors. This has resulted in the emergence of several existing threats, including [7]:

Increase in Cyberattacks: In the modern era, cyberattacks have evolved and taken on various forms. Ransomware, Advanced Persistent Threats (APT), Phishing, and Man-In-The-Middle (MITM) attacks present serious threats to organizations and individual users. These attacks aim to steal or destroy data or disrupt an organization's operations, leading to significant financial losses and data breaches.

Cloud Security: Organizations store their data through cloud services, which complicates issues related to data storage location and control. Security concerns in cloud environments primarily involve data encryption, access control, and application control [1].

Internet of Things (IoT): System vulnerabilities and integrity issues associated with IoT devices pose a significant threat. The increasing number of connected devices in networks opens new avenues for attacks. IoT devices, with their weak security measures and open network ports, can create serious security risks.

Data Loss and Theft: This threat arises from both technological failures and human factors (user mistakes and internal threats). The absence of Data Loss Prevention (DLP) technologies and weak password practices by users increase these risks.

References

[1] Məmmədov, F. "Bulud texnologiyalarında məlumat təhlükəsizliyi və əlçatanlıq." Yeni Texnologiyalar və Təhlükəsizlik Jurnalı. **2022**, 10(1), 45-56.

[2] İsmayılov, R. "İnformasiya təhlükəsizliyində yeni yanaşmalar: Kriptoqrafiya və şəbəkə təhlükəsizliyi." Təhlükəsizlik və İnformasiya Texnologiyaları Jurnalı. **2021**, 5(2), 110-118.

[3] Əhmədov, T. "İnformasiya təhlükəsizliyində siyasət və idarəetmə." Azərbaycanın İnformasiya Təhlükəsizliyi Jurnalı. **2020**, 4(2), 56-65.

[4] Xəlilov, F. "İnformasiya təhlükəsizliyi və əlçatanlıq: Post-kvant şifrələmə yanaşmaları." Kriptoqrafiya və Təhlükəsizlik Jurnalı. **2021**, 9(3), 78-86.

[5] Barrett, A., & Rowe, D. "Privacy and Access Control in Distributed Systems." Journal of Cyber Security Technology. **2022**, 6(4), 215-234.

[6] Jiang, P., & Liu, H. "Machine Learning in Cybersecurity: A Survey of Applications, Trends, and Challenges." Computers & Security. **2023**, 114, 101718.

[7] Panda, P., & Sharma, S. "The Future of Cryptography in Securing Information Access Control." Journal of Information Security. **2023**, 22(2), 129-145.

[8] Xie, J., & Li, Z. "Zero Trust Security Models for Cloud and Distributed Systems." IEEE Access. **2022**, 10, 11109-11118.

[9] Yang, Q., & Xu, W. "Improved Role-based Access Control Models for Cloud Services." Journal of Cloud Computing: Theory and Applications. **2023**, 12(2), 101-115.

[10] Hassan, N., & Zhang, L. "Blockchain Technology for Secure and Efficient User Access Control in Distributed Systems." Computers, Materials & Continua. **2021**, 68(2), 1629-1641.

[11] Курочкин, С. В. "Безопасность информационных систем." Журнал информационных технологий. **2022**, 15(3), 120-130.

[12] Смирнов, Д. В. "Управление доступом в распределённых информационных системах." Технологии информационной безопасности. **2020**, 10(1), 45-52.

[13] Чистяков, В. О. "Методы защиты информации и криптографические стандарты." Журнал защиты информации. **2021**, 7(4), 101-110.