eISSN: 2229-3213 pISSN: 2229-3205
The Journal of Applied Science and Social Science
Volume 16,Issue 04 April, 2026

INTEGRATION OF CRYPTOGRAPHIC AND ACCESS CONTROL SYSTEMS IN ENSURING INFORMATION SECURITY

G'ulomova Ko'hinur Murod qizi
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Ko'chimova Oyshabonu O'tkirjon qizi
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Usmonov Faxriddin Sharofiddin o'g'li
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
Muhammatjonov Muxammadqodir Rashidbek o'g'li
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotation

This article examines cryptographic algorithms, access control models, and processes, as well as their interrelationship in ensuring information security. It highlights how these components work together to protect data, manage access, and maintain system integrity in modern information systems.

Keywords

security, cryptography, confidentiality, integrity, data integrity, DAC, MAC, RBAC, ABAC, identification, authentication, authorization, auditing, LDAP, symmetric key, asymmetric key, digital signature

Introduction

Today, along with the rapid development of information technologies, cybersecurity issues are becoming increasingly relevant. For every organization, enterprise, or government system, protecting information resources is considered one of the most important tasks. The primary goal of information security is to ensure the confidentiality, integrity, and availability of data. In this context, cryptography and access control technologies play a crucial role, as they are essential components of the security infrastructure of information systems.

Cryptography protects data from unauthorized access by encrypting it and ensures user authentication. Access control systems, on the other hand, regulate who can access information resources, when, and to what extent. These two mechanisms are closely interconnected: one protects the data itself, while the other manages access rights to it. In modern networks, the growing number of users, along with the widespread use of cloud technologies and mobile devices, makes the integration of these two areas even more important.

Therefore, studying the interrelationship between cryptographic methods and access control mechanisms in ensuring information security, as well as developing an integrated approach for their effective implementation, is an important scientific and practical task. This article is devoted to analyzing this issue and examining their interdependence.

About Cryptographic Technologies

Cryptography studies mathematical methods related to the key objectives of information security, including confidentiality, data integrity, entity authentication, and message authentication. It is not only a tool for ensuring information security but also a comprehensive set of methods and techniques used to protect data and secure communication systems.

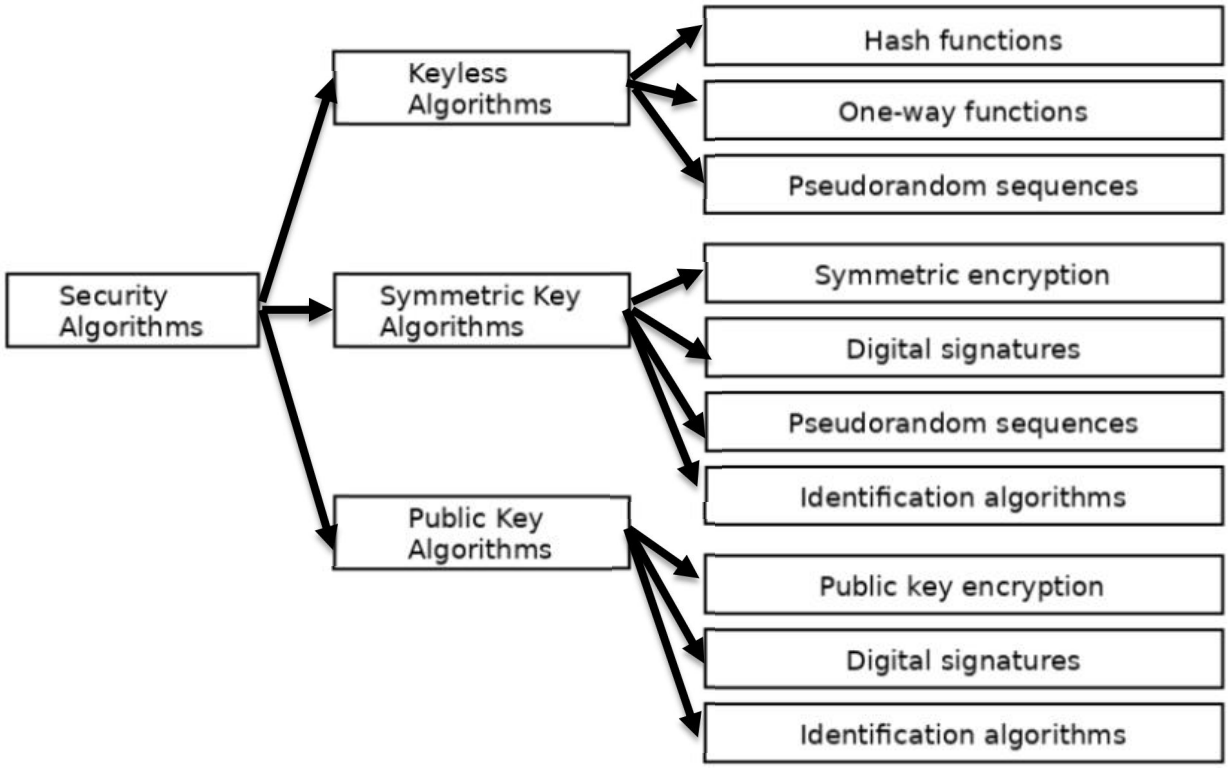

Figure 1. Cryptographic Algorithms

Relevance of DDoS Attacks and Protection Systems

Distributed Denial of Service (DDoS) attacks have significantly increased in recent years in terms of volume, scale, distribution, and complexity, as evidenced by record-breaking attacks. Unfortunately, many organizations still rely on outdated assumptions about their protection-believing that their defenses are sufficient or that they are unlikely to become targets. In reality, victims of such attacks include all major sectors, from financial services and e-commerce to online gaming. In particular, attacks on critical national infrastructure-such as healthcare, energy, utilities, education, and transportation-are of serious concern.

For example, in 2023, Akamai protected a customer in the Asia-Pacific region from a massive 900 Gbps attack. Later that year, it mitigated a 634 Gbps, 55 million packets per second (Mpps) attack involving a complex mix of attack vectors-one of the largest attacks against a U.S. financial services client. These were preceded by an even larger global attack reaching 1.44 Tbps and 385 Mpps, lasting nearly two hours. These incidents clearly demonstrate that cybercriminals continue to target critical sectors of the economy.

Although the scale of such attacks may lead smaller organizations to believe they are unlikely targets, the reality is that critical services and applications in every industry are vulnerable. The increasing number of hackers driven by political or ideological motives, along with the affordability of "DDoS-as-a-service" offered by groups such as Killnet and Anonymous Sudan, makes almost any organization a potential target.

Moreover, DDoS attacks are increasingly used as a distraction technique to overwhelm network and security resources, while attackers simultaneously attempt other malicious activities such as ransomware DDoS (RDDoS) or multi-layer extortion campaigns. The growing use of artificial intelligence tools to organize sophisticated and distributed DDoS attacks poses additional challenges for enterprises and government institutions that must ensure continuous availability and performance.

As threats become more complex and evolve rapidly, many myths about DDoS

protection still persist—some even promoted by security vendors. Therefore, DDoS protection must be a fundamental component of any cybersecurity strategy, and understanding these misconceptions is critical for effective defense.

DDoS Protection Capacity Considerations

Total capacity indicates the overall volume of mitigation resources available. However, relying solely on network capacity figures can be misleading, as it may omit critical details. Organizations evaluating DDoS protection solutions should consider the following questions:

- How much of the network capacity is dedicated specifically to absorbing attack traffic?
- What portion of mitigation resources is allocated to stopping active attacks?
- How much network and system capacity is available to deliver clean traffic to each customer and tenant?

These questions are important because if total network capacity also serves other functions-such as content delivery-the actual DDoS mitigation capability may represent only a fraction of what is claimed by the provider.

DDoS defense is not limited to technology alone. When automated systems reach their limits, are there sufficient human resources available for escalation, incident response, and fine-tuning? The most reliable mitigation solutions combine automation and machine intelligence with human expertise to provide layered defense.

Relevance of Developing Protection Systems Against Denial-of-Service Attacks

The importance of developing systems to protect against denial-of-service threats is determined by several key factors:

Today, information technologies have penetrated all areas of life, increasing dependence on information resources. While the widespread use of the internet and digital technologies has expanded access to information, it has also intensified cybersecurity threats. Cybercrimes-including DDoS attacks, hacking, and other forms of cyberattacks-are steadily increasing. These attacks can lead to system failures, data loss, or data theft.

At the global level, geopolitical tensions are increasing the risk of cyber warfare and information warfare. States and other actors may attempt to harm their opponents by disrupting access to information resources. Information freedom is a fundamental principle of democratic societies, and restricting access to information can hinder social development and violate freedom of speech.

Denial of access to information can also cause significant damage to business operations, financial systems, and economic sectors. Cyberattacks can result in losses amounting to millions of dollars for companies. In addition, the protection of personal data has become critically important, as unauthorized access may lead to data theft or exposure.

Table 1

Core Technologies of Access Control

Texnologiya nomi	Vazifasi	Qayerda qo‘llaniladi
LDAP (Lightweight Directory Access Protocol)	Foydalanuvchi identifikatsiyasi va ma’lumotlar katalogini boshqarish	Active Directory, Linux tarmoqlari
Active Directory (AD)	RBAC asosida markazlashgan foydalanuvchi boshqaruvi	Korporativ Windows tarmoqlari

Kerberos	Tarmoqda foydalanuvchini ishonchli autentifikatsiya qilish	Server–klient tizimlarda
RADIUS / TACACS+	Tarmoq qurilmalarida foydalanuvchi kirishini nazorat qilish	Router, switch, VPN tizimlarida
OAuth 2.0 / OpenID Connect	Veb-ilovalar va API-lar uchun avtorizatsiya protokoli	Google, Facebook login tizimlari
Zero Trust Architecture (ZTA)	Har bir kirish harakatini doimiy tekshiruvchi xavfsizlik modeli	Bulutli va korporativ muhitlarda
SAML (Security Assertion Markup Language)	Turli tizimlar orasida autentifikatsiya ma'lumotlarini almashish	Single Sign-On (SSO) tizimlari

LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol) is a directory protocol used to manage and access information stored in a directory. Although LDAP is most commonly used in enterprise environments with Microsoft Active Directory Domain Services (AD DS), it is a vendor-agnostic protocol that can be used with many different types of user directories.

LDAP was created in 1993 as a lightweight alternative to the existing X.500 directory service protocols. The X.500 protocols required significant computational power and bandwidth, making them resource-intensive compared to their successor, LDAP. Now, more than 30 years later, LDAP is widely used for various purposes.

Because LDAP can query directory data, it can be used for Single Sign-On (SSO), where an existing account in the directory is used to authenticate a user to an application or service. Although newer protocols such as OAuth2 and SAML are widely used in modern SSO implementations, LDAP is still commonly used in many enterprise environments to provide SSO capabilities.

In addition to authentication, LDAP can be used to retrieve directory information such as user attributes (e.g., name, department), group membership, employee identifiers, access control lists, and more. Depending on the level of access, LDAP can also be used to update the directory by adding, deleting, or modifying entries.

How LDAP Works

LDAP operates as a query-based protocol that allows services and applications to retrieve user information from a directory. This process consists of four main steps:

1. Session Connection – The service or application connects to the LDAP server via a designated port.
2. Request – The user or application sends a query to the server, typically using a user identifier or email.
3. Response – The server processes the request, retrieves the relevant information, and returns it to the user.
4. Completion – The connection to the LDAP server is closed.

These steps remain the same regardless of the use case, as the primary purpose of LDAP is to efficiently provide directory information.

LDAP Infrastructure Requirements

Although LDAP is widely supported, it requires a specific infrastructure to function properly. To implement LDAP within an organization, the following components are needed:

- Directory Server – Typically a Microsoft Active Directory instance running on a domain controller. LDAP services must be enabled and configured here.

- LDAP User Account(s) – An account is required to authenticate to the LDAP server. This account must be securely protected, as it can query the entire directory, including sensitive data.
- Directory Data – The directory must contain data for LDAP queries, such as user accounts, groups, and computer objects.
- LDAP Client – A system or application configured to query directory data using LDAP.
- LDAP Security – Although optional, security protocols should be used to protect directory data. Most organizations use SSL (Secure Socket Layer) or TLS (Transport Layer Security) to ensure confidentiality and integrity of LDAP traffic.

LDAP Usage in Applications. Once the LDAP infrastructure is set up, any service or application that supports LDAP can be configured to use it for authentication or directory queries. This is done by connecting to the LDAP server using an LDAP user account.

Depending on the use case, the connection may be:

- Persistent (long-term) – For example, when continuously authenticating users, the application frequently queries the LDAP directory.
- Temporary (short-term) – The connection is established, a query is performed, and then the connection is closed.

In all cases, the LDAP account used for the initial connection must be reused whenever the service or application needs to communicate with the LDAP server.

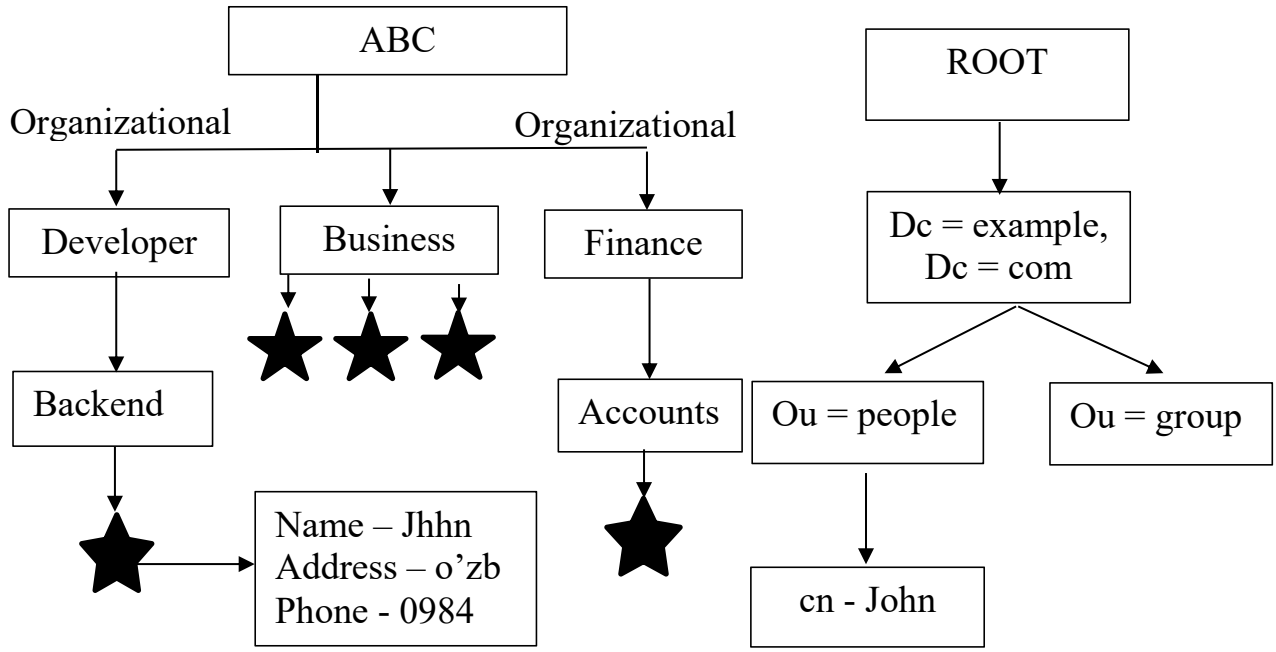

Figure 2. LDAP Structure

LDAP Directory Structure and Attributes

In this context, the asterisk (*) represents a user. Similar to other directories such as Active Directory, LDAP servers organize data in a hierarchical tree structure. The top level of the directory is typically called the root, which represents the owning organization.

The next level is usually the domain, and if an organization uses multiple domains to structure its user base, the root branches out accordingly.

The way information is organized depends on how the enterprise structures its directory. However, after the domain level, it is common to see data objects divided into categories such as

users, groups, computers, and sometimes additional attributes like departments.

There are several terms used to describe the location of an object in an LDAP directory:

- Organizational Unit (OU) – An OU can be thought of as a subfolder within the directory hierarchy. For example, a user named John Doe may be located in the *Users OU*, which is subordinate to *exampledomain.org*.
- Distinguished Name (DN) – Similar to an address, this is a unique identifier that describes where an object is located within the directory. Using the example above, John Doe's distinguished name would be:

cn=John Doe, ou=Users, dc=exampledomain, dc=org

LDAP Attributes

In addition to defining object locations, LDAP directories use attributes to describe object properties. These may include first name, last name, job title, department, and phone number.

Some of the most commonly used attributes include:

- cn (Common Name)
- dc (Domain Component)
- description
- displayName
- dn (Distinguished Name)
- givenName (First Name)
- mail (Email Address)
- ou (Organizational Unit)
- sn (Surname / Last Name)
- telephoneNumber
- userPrincipalName (UPN) – Similar to an email address, but used to identify the domain of the object (e.g., *johndoe@exampledomain.org*)

Relationship Between Cryptography and Access Control

Two fundamental pillars of information security - cryptographic protection and access control systems - are complementary technologies that support each other.

- Access Control determines the identity of a user and defines which resources they are allowed to access (Authentication + Authorization).
- Cryptography protects data by encrypting it, ensuring that even if unauthorized access occurs, the content remains secure (Confidentiality + Integrity).

Their interrelationship is reflected in the following aspects:

- Data remains encrypted until access is properly authorized
- Decryption is only available to authorized entities
- Key management processes operate in alignment with access control policies
- The reliability of audit, identification, and authentication processes is ensured through cryptographic protocols (e.g., TLS, Kerberos)

Conclusion

Ensuring information security is one of the most critical tasks in today's digital environment. The vast amount of data generated and exchanged by organizations and users requires a comprehensive approach to protection.

In this process, cryptographic technologies and access control systems serve as complementary core mechanisms. Cryptography ensures confidentiality, integrity, and authenticity of data through encryption, while access control restricts system resources only to authorized users.

When these technologies are applied together, they create a strong, multi-layered defense against security threats. For example, even if access control is compromised, cryptography can

still protect the content of the data. Additionally, key management, authentication, and audit processes rely on access control policies.

As a result, the reliability and stability of the system are significantly improved.

In conclusion, the integration of cryptography and access control technologies is one of the most effective and essential requirements for securing modern digital infrastructures.

References

1. Stallings, W. *Cryptography and Network Security*
2. Pfleeger, C. P. *Security in Computing*
3. NIST SP 800-53 – *Security and Privacy Controls for Information Systems*
4. RFC 4949 – *Internet Security Glossary*
5. Law of the Republic of Uzbekistan “On Information Security” (2019)