[4] Coyne, E. J., & Davis, J. M. (2017). Role engineering for enterprise security management. Information Systems Security.
[5] Ferraiolo, D., Kuhn, R., & Chandramouli, R. (2014). Role-Based Access Control. Artech House.
[6] Gupta, P., & Seetharaman, A. (2019). The Business Impact of Role-Based Access Control: A Systematic Literature Review. Expert Systems with Applications.

MANAGING ACCESS IN DISTRIBUTED SYSTEMS: OVERVIEW

Tural Ahmadov , Kifayyat Mammadova

Abstract
This review provides a comprehensive analysis of access management (AM) methods in the field of information security. AM is a key aspect of protecting sensitive data and resources from unauthorized access. Understanding various AM models and mechanisms is crucial for designing effective security solutions. One of the main goals of the study is the diversity of AM approaches, analyzing models from traditional discretionary AM (DAM) and mandatory AM (MAM) to more newly developed models such as role-based AM (RBAM), attribute-based AM (ABAM), and policy-based AM (PBAM). Additionally, enforcement mechanisms like AM Lists (AML) are discussed. This research work is proposed as a valuable resource for researchers, practitioners, and administrators involved in information security and AM decision-making.
Keywords: access management; distributed systems; information security.

Introduction

In modern society, many digital innovations have transformed organizations and altered their operational structures, leading to the establishment of internal networks and connections to broader networks. The evolution of networks has provided businesses with efficient and effective communication solutions that require advanced Authentication and Authorization solutions for the storage of data [1]. Access Management (AM) is a solution to address information security issues by fulfilling specific security requirements to prevent unauthorized access to various resources. Since AM is a very active research field, this scientific work aims to explore existing technical solutions and application areas by examining issues surrounding reliable digital transformation strategies for organizations and enterprises.

Background and related work

AM is a valuable technique for protecting information security by determining who or what can see or use resources. According to the definition provided by NIST for AM [2]:
A usually automated set of procedures or processes that allow access to a particular space or data managed in conjunction with predefined policies and rules.'AM is considered the foundation of information security in fields including Cloud Computing and the Internet of Things. AM has the capability to monitor access to resources and effectively prevent unauthorized data flows [3].
According to Stallings and Brown [4], AM solutions can be designed with three main principles in mind:

–Identification - The process of verifying the correctness of specific access credentials of the user (subject) and various system objects.

–Authorization - The process of granting or denying access permissions for a system resource (object), deciding for what purpose the subject is trusted.

–Audit - An independent review that checks system logs or activities to understand the status of system management tools. Additionally, conducting an audit can help ensure compliance with established policies and operational procedures, detect security breaches, and provide recommendations for improving Information Security Management Systems (ISMS).

Subjects are held accountable for their actions. There are various established classes of users (subjects) with different access rights. For example:

–Owner - The creator of the resource (file).

–Group - A group of users with specific access rights in addition to the owner.

–World - Users who cannot access the system and are excluded from the owner or group categories for resources.

–Access rights - Determine how subjects can access objects.

Examples:

–Read - The subject can view the data in the object. The ability to copy and print is included in the "read" permission.

–Write - The subject can modify or delete the data in the object.

–Execute - The subject can execute specific programs.

–Delete - The subject can delete specific objects such as files or records.

–Create - The subject can create new files, records, or fields.

–Search - The subject can list the files in the directory and search the entire directory.

AM systems can be centralized or decentralized [5]:

–Centralized AM allows subjects to access each application, website, and specific computing resource from a single profile using precise access credentials available everywhere. Additionally, all data assets controlled by the user are under unified identification management.

–Decentralized AM eliminates the need for a specific administrator to manage or grant access to specific users on certain software or online platforms. Additionally, users do not necessarily control their access credentials. For example, in Bitcoin, encryption keys are automatically generated and associated with the account.

This research [6] identifies issues related to the implementation of AM in distributed architectures where some systems were not designed to accommodate AM. Specifically, it examines the tension caused by overly stringent rules and the severe risk of data loss due to excessively permissive sharing. Managing authentication can also be challenging due to weak coordination between independent systems.

AM solutions

In this section, I highlight various Access Management approaches (Discretionary, Mandatory, Attribute-based, Role-based, and Policy-based) and their applications (Group Policies), alongside standard enforcement mechanisms (AM Lists and Matrices, Capability Lists).

AM List (AML). The AM List consists of rules for granting or denying access to specific resources. It is managed by one or more Access Permissions Management Entities (APMEs) that determine rules for special users or security identifiers. New entries are typically added to the end of the AML. AMLs can be implemented in various domains, for example, through programs or devices such as Triple Content-Addressable Memory (TCAM) [7] to accelerate query processing in File Systems and Networks. AMLs can be applied in various operating systems, including popular ones like "Linux" and "Windows" demonstrating agility as a security measure for systems and infrastructures.

Capacity List (CL). The capability list can be a token or ticket that grants access to objects in the computer system to the subject. Before granting access to a specific object, the subject is evaluated with the capability list.

AM Matrix. The AM can be generalized to the AM matrix. According to Huang and others [8], the mechanism is implemented as an array of columns for each object and an array of rows for each subject. The letters in a particular cell indicate the access permission for the corresponding objects for the subject. Columns represent the permission list for the object; a row is equivalent to the permission profile of the subject (see Table 1).

Table 1. AM matrix

User	File 1	Fayl 2	Fayl 3	Printer
John	W	R	R	OK
Emin	R	RW	W	
Melisa	RW			OK
Ruslan	R	W	R	
Abdul			RO	OK

Group Policy. Group Policies are a feature specific to operating environments such as "Microsoft Active Directory" which have authority over subject accounts in the working environment, including distributed environments like "UNIX" and "Microsoft Windows" operating systems. Group Policies provide centralized management and configuration for operating systems, user settings, and applications to enable effective AM implementation. As discussed by Sampeman and others [9], Group Policies can be utilized when various users interact with the AM system. Within a group, users share common permissions. Describing the ability to add new policies to the Group Policy, it is then implemented to multiple users, desktop computers, and servers through Active Directory.

Discretionary AM (DAM). The Authorization mechanism that assesses the identity of the requester or enforces access rules (permissions) to restrict access to a desired AM object using trusted evaluation criteria provided by reliable computer systems is referred to as Discretionary AM (DAM). DAM is implemented by using AM systems, where a reliable AM solution is considered when the number of users and resources is limited. DAM is the most common AM solution for operating systems such as "Windows" and "UNIX." However, as discussed by Gagandeep and Arvinder [10], it presents several conflicts in cloud-based environments. Firstly, it complicates the management of processes at the administrator level. Secondly, granting access to objects to other users by the object owner may pose security issues. Thirdly, it plays a complex audit role. Tracking information in the DAM system is challenging because it is not a centralized system; it only allows administrators to control the local flow of each AM.

Mandatory AM (MAM). Mandatory Access Management (MAM) is often used in institutions with serious security requirements, such as governments and public services. MAM manages access by comparing security labels that indicate the sensitivity or criticality status of system resources. This involves creating different security formalization levels and associating system objects with one of these security levels. In practice, each object can be assigned labels such as Unclassified, Confidential, Secret, or Top Secret. Access higher than the subject's own clearance level is not permitted.

Attribute Based AM (ABAM). In Attribute-Based Access Management (ABAM), access and authorization are determined based on attributes associated with the subject and the requested object. All objects and subjects possess a set of relevant attributes such as Location, Creation, and Access Rights. Access to objects is granted or denied based on the compatibility between object and subject attributes.

Role Based AM (RBAM). Role-Based Access Management (RBAM) provides access and authorization based on user roles. It grants subjects specific permissions for a particular role, both implicitly and explicitly. Role permissions are inherited using role hierarchies and determine the permissions required to perform specific operations. Specific roles can be assigned to one or multiple users. Unlike other AM solutions, RBAM can be utilized at the enterprise level to create security policies that go beyond the capabilities of AM systems, which determine how users can modify files.

Future research in the field of AM. One potential future research topic could be the examination of existing and newly developed mechanisms related to security in the "Microservices architecture" which has gained popularity in the last decade and has become an active research area in web programming. In this research, I investigated the management of appropriate access permissions for users to access resources using various mechanisms at different levels of the AM. In the "Microservices architecture" managing access permissions across software systems, exploring various existing and emerging methods could be further explored. This may involve processes such as authentication and authorization, assigning keys, usage of refresh tokens, utilizing "JWT" tokens, and other subtopics related to inter-system authentication and authorization processes.

Conclusion

This research provides a comprehensive overview of AM methods in the field of information security. Through analysis of various AM models, mechanisms, and technologies, we have gained insights into the evolving mechanisms of AM and its importance in safeguarding sensitive information and resources. One of the main findings of this overview is the diversity of AM approaches, ranging from basic Discretionary AM (DAM) and Mandatory AM (MAM) models to more recently developed role-based AM (RBAM), attribute-based AM (ABAM), and policy-based AM (PBAM) models. Each approach offers unique advantages and limitations, and the choice of AM model should be tailored to the specific requirements and security objectives of the system or organization. As a future research endeavor or as an extension to this study, efforts can be directed towards analyzing information security approaches in the rapidly evolving field of "Microservices architecture" which represents one of the most modern examples of distributed systems. In conclusion, the findings of this overview highlight the significant role of AM in ensuring the confidentiality, integrity, and availability of information. By understanding the strengths and limitations of different AM approaches, organizations can develop robust AM strategies that align with their security requirements and business objectives. As technology continues to evolve, ongoing research and advancements in the field of AM will be crucial to adapting and safeguarding against increasingly interconnected and data-driven threats, as well as protecting against unauthorized access.

References

[1] S. Drame-Maigne, M. Laurent, L. Castillo, H. Ganem, Centralized, distributed, and everything in between: reviewing access control solutions for the IoT, ACM Computing Survey, v. 54, is. 7, p. 1-34, (2021), doi:10.1145/3465170.

[2] National Istitute of Standards and Technology, Access Control, Computer Security Resource Center, Qeytersburq, (2024), url:https://csrc.nist.gov/glossary/term/access_control.

[3] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, B. Fang, A survey on access control in the age of internet of things, IEEE Internet of Things Journal, v. 7, is. 6, p. 4682-4696, (2020), doi:10.1109/JIOT.2020.2969326.

[4] V. Stallings, L. Brown, Computer Security: Principles and Practice, Pearson Education Limited, p. 134-158, (2018), url: http://refhub.elsevier.com/S2772-9184(23)00003-6/sbref0003.

[5] T. Cerny, A. Walker, J. Svacina, V. Bushong, D. Das, K. Frajtak, M. Bures, P. Tisnovsky, Mapping study on constraint consistency checking in distributed enterprise systems, Proceedings of the International Conference on Research in Adaptive and Convergent Systems, p. 167-174, (2020), doi:10.1145/3400286.3418257

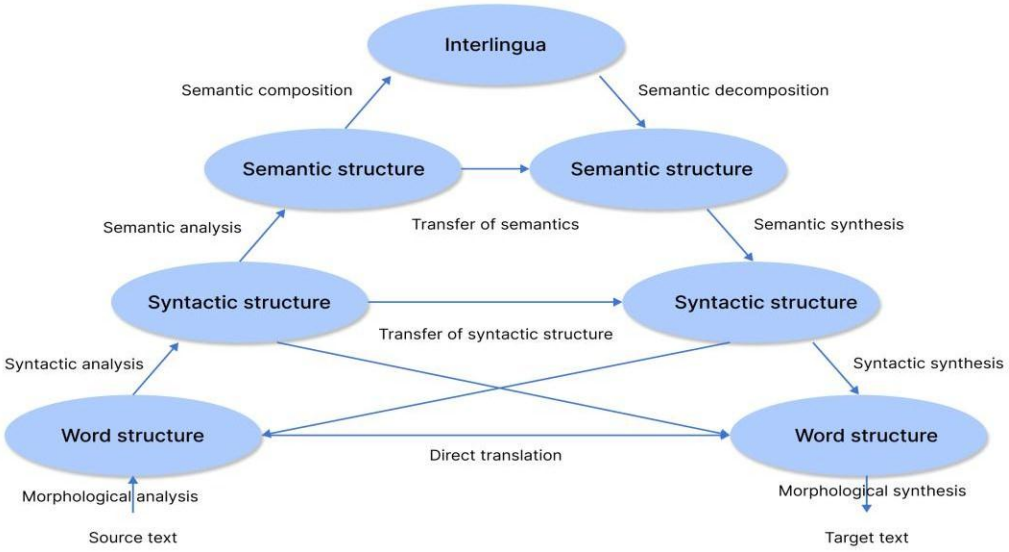
[6] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, Access control for emerging distributed systems, Computer, v. 51, is. 10, p. 100-103, (2018), doi: 10.1109/MC.2018.3971347.

[7] Y. Sun, M. S. Kim, Tree-based minimization of TCAM entries for packet classification, 7th IEEE Consumer Communications and Networking Conference, p. 1-5, (2010), doi:10.1109/CCNC.2010.5421589.
[8] Yin-Tzu Huang, Dai-Lun Chiang, Tzer-Shyonq Chen, Sheng-De Wang, Fei-Pei Lai, Yu-Da Lin, Lagrange interpolation-driven access control mechanism: towards secure and privacy-preserving fusion of personal health records, Knowledge-Based Systems, v. 236, (2022), doi:10.1016/j.knosys.2021.107679.
[9] G. Sampemane, P. Naldurg, R. H. Campbell, Access control for active spaces, 18th Annual Computer Security Applications Conference, p. 343-352, (2002), doi:10.1109/CSAC.2002.1176306.
[10] G. Kaur, Sh. Garg, Performance Evaluation of OFDM System for Different Modulation Techniques on the basis of Bit Error Rate and Peak to Average Power Ratio, Foundation of Computer Science FCS, v. 1, is. 2, p. 32-36, (2015), doi:10.5120/cae-1508.

MACHINE TRANSLATION APPROACH AND ITS CONCEPTS

Hummatova Sulhana, Haciyev Yashar
Azerbaijan State Oil and Industry University ,Applied Linguistics, Computer Engineering

Abstract
İn this article, machine translation, its concepts, and algorithmic principles are established. İt is a machine translation (MT) approach based ona set of linguistics rules and dictionaries to translate text from one language to another.Updates should be made to the program to eliminate translation errors.
Key Words : Machine translation, Interlingua, Statistical approach , Hybrid MT.
Introduction: Machine translation is the process of using artificial intelligence to automatically translate text from one language to another without human intervention. Modern machine translation programs go beyond simple word-by-word translation and convey the full meaning of the source text. Also, it analyzes all the elements of the whole text and recognizes how the words affect each other.
Translation whether machine or human, comes with a cost which can be divided into three segments. Firstly, the linguistics knowledge of particular languages involved. Secondly, theoretical frameworks for the system to be constructed and finally, the programming skills.The actual cost of each segment depend on the methodology used to implement the translation. The first successful experiment was the Georgetown |University experiment, which was a joint project of this university and IBM in 1954. Thus, the experiment consisting of 6 grammatical rules and 250 words in memory gave successful results and increased the hopes for the development of the science field of machine translation.
Since the 21st century is the age of computers, computerization of every field involving all available human labor is gaining momentum. Electronicization was becoming widespread in every field, it may be medicine, language or technology. For this reason, online translation programs were preferred for human translations. Thus, it became possible to carry out any kind of translation in the shortest time without paying any additional funds or effort. Bernard Vauquois gave a machine translation model with his triangle, known today as the Vaugois triangle. The Vauqois triangle explains and visualizes the machine translation model and shows its approaches.



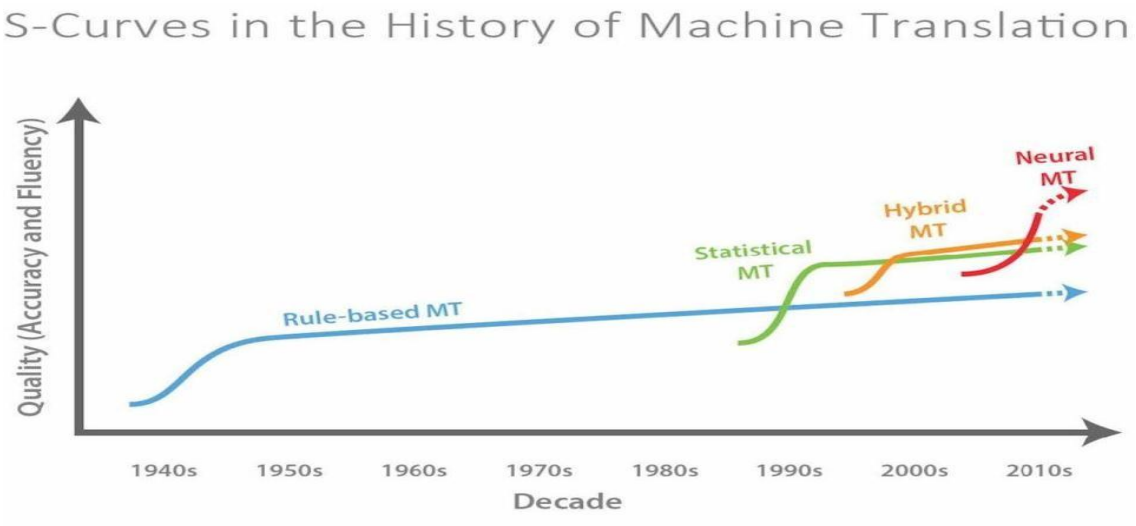
Machine Translation Model (Bernard Vauquois)

The direct translation approach uses a bilingual dictionary to translate sentences word by word. Here each source word is combined with some target words. The translation process does not use any intermediate structures other than some morphological analysis (it makes analyzing the structure and parts of words) and lemmatization (the task of converting a word into its basic lexical form, such as translation).After analyzing the sentence structures and parts, each word is matched to a word in the target language and translated words for use in the target language. Some simple reordering operations are performed on the resulting target language sentences are correct.

The transfer-based translation approach first determines the sentences in the source language by breaking them into parts, applies the rules for partial transfer into the target language to create the resulting structure from the knowledge of the difference between languages, and then produces the target language sentences from this transformed sentence structure. Their changes may vary depending on their source and variability. For similar languages, cognate languages are almost 80-90% lexically identical but only syntactical differences are possible.

İnterlingua-With This method, which is the highest level of analysis is used from the source languages. A meaningful analysis of the representation results in an abstract language. The necessary parsing of the source language expression is generated regardless of the language that can be created. This abstract language is parsed in the target language. Machine translation engines are complex systems with a deep history and evolutionary process. These systems are created by expert linguistics and technicians using algorithms, codes and decoding. A very classical approach has beeen adopted in rule-based machine translation. This approach is based on linguistics information gathered from dictionaries and linguistics source and target languages.

İn the 1990s, machine translation üas replaced by statistical machine translation. Statistical machine translation analyzes bilingual texts and data.This was an important step for rule-based machine translation, as machines learn grammar rules spontaneously without needing the help of linguists. Although statistical machine translation is considered a more traditional translation model, it is still useed today.Over time the development of machine translation has given rise to different types of machine translation systems despite their strength and weaknesses. The most common types of machine translations are rule-based machine translation, statistical machine translation, neural translation, and hybrid machine translation.



The oldest form of effective machine translation, rule-based machine translation relied on a board, a predefined set of linguistic rules that helped software convey the meaning of text between languages. Overall translation quality was poor and required a significant amount of human post-editing and manual addition of languages. SMT was used for machine translation approaches in the 1990s. And it gave great results for next translation programs.SMT is a data-driven approach which uses parallel aligned corpora and treats translation like a mathematical problem in that every target language is a translation as a mathematical reasoning problem. The higher the probability is the higher accuracy of translation. Although statistical methods still dominate research in machine translation, most commercial machine translation systems are rule-based. Recently the boundaries between these two approaches have narrowed and hybrid approaches that try to benefit from both have emerged. We distinguish two groups of hybrid MTs: those driven by rule-based MTs and statistical methods. Hybrid MT formula can be characterized as follows:

$$HMT=SMT+RBMT$$

So in this both statistical and RBMT method are used as shown in formula.Recently wide used approach is neural machine translation has 2 main components, which are encoder and decoder. Here the encoder converts the sentences in the source language into a real value vector. This method seems closer to human translation. Neural translation analyzes the available data directly and gets the appropriate result.

Conclusion

The article provides an overview of current machine translation approaches developed from 1940 and developed a classification structure based on basic features for example: data, rules, or both of them**.** There is a need in rule-based and statistical machine translation methods for teaching the computer the language rules, a good dictionary and collection. Lack of bilingual rich dictionaries, improved written and oral collections leads some languages to be put at disadvantage in the machine translations.

References:

[1] Nabiyev, V.V. Yapay Zeka, Seçkin Yayıncılık 2016
[2] Lopez A. Statistical machine translation 2008
[3] Antony P J. "Machine Translation Approaches and Survey for Indian Languages." 2013

[4] Murphy, G., The Big Book of Concepts, Cambridge 2002
[5] Papineni, K., Roukos, S., Ward, A Method for Automatic Evaluation of Machine Translation 2002
[6] Ralf D. Brown. Context-sensitive retrieval for example-based machine translation-2015
[7] Masterman, M., The Thesaurus in Syntax and Semantics, Mechanical Translation 1957
[8] Sowmya Vajjala , Anjuy Gupta "Practical Natural Language"
[9] https://en.wikipedia.org/wiki/Rule-based_machine_translation

NDVİ İNDEKSLƏRİ VASİTƏSİLƏ HƏKƏRİ ÇAY HÖVZƏSİNİN QUBADLI, ZƏNGİLAN VƏ LAÇIN RAYONU ƏRAZİLƏRİ ÜZRƏ SULU VƏ SUSUZ TORPAQ ƏRAZİLƏRİNİN EKOLOJİ VƏZİYYƏTİNİN QİYMƏTLƏNDİRİLMƏSİ VƏ MÜQAYİSƏLİ TƏHLİLİ

Məmmədəliyeva V.M. Nəsirova V.R.
MAKA Ekologiya Institutu

Abstract
NDVİ indeksləri vasitəsilə həkəri çay hövzəsinin Qubadlı, Zəngilan və Laçın rayonu əraziləri üzrə sulu və susuz torpaq ərazilərinin ekoloji vəziyyətinin qiymətləndirilməsi və müqayisəli təhlili mövzusunda aparılan tədqiqatdır . Laçın, Qubadlı və Zəngilan rayonlar ərazisində susuz və sulu artan və azlan sahələrini təyin edərək meşə-bitki örtüyünün peyk məlumatlar əsasında baş verən dinamikasını təyini etməkdən ibarətdir. Meşə-bitki örtüyündə baş verən dəyişikliyini müəyyən etmək üçün tədqiqatı əsasən sulu torpaq və susuz (quru) torpaq sahələrini araşdırılmış, bundan əlavə artan, azalan və sabit növlərinə ayrılmışdır. Beləliklə susuz topraq ərazilərin artması zamanı meşə-bitki örtüyünün vəziyyətini nəzərdən keçirilmişdir. Beləliklə apardığımız tədqiqat işində susuz torpaq sahələrin artması ərazinin əsas hissəsi güclü sıx bitki örtüyü (kolluqlar) sahələrin azalması, kolluqlar və otlaq sahələrin artması baş vermişdir, digər tərəfdən susuz torpaqların azalması ən böyük sahəni kolluqlar və otlaq olmaqla azalma, meşəsiz ərazilərin azalması, çılpaqvə seyrəlmiş ağac və kol bitkilərin artması baş vermişdir. Lakin sulu torpaq sahələrin artması zamanı əsasən dağ növləri, qum, qar, meşəsiz ərazilərində, kolluqlar və otlaq sahələrin azalmasında, çılpaq və seyrəlmiş ağac və kol bitkilərin kəskin artmasında baş vermişdir, sulu torpaq sahələrin azalması zamanı kolluqlar və otlaq sahələrin kəskin artması, güclu sıx bitki örtüyü (kolluqların) isə kəskin azalması baş vermişdir.
Açar sözlər: NDVİ indeksi, ENVİ, susuz və sulu sahələr, dinamika, artan və azalan sahələr
Məqsəd. Laçın, Qubadlı və Zəngilan rayonlar ərazisində susuz və sulu artan və azlan sahələrini təyin edərək meşə-bitki örtüyünün peyk məlumatlar əsasında baş verən dinamikasını təyini etməkdən ibarətdir.
Metodlar. Burada əsasən 2000 və 2021-ci illərin Landsat-5 və Landsat-8 peyk məlumatlardan istifadə edərək ArcGİS və ENVİ proqram təminatından istifadə edərək NDVİ və MNDWI indeksindən istifadə edərək emal aparılmışdır.
Laçın rayonu əsasən çimli, dağ-çəmən, qəhvəyi dağ-meşə və karbonatlı dağ qara torpaqlara malikdir. Bitki örtüyü kollu və seyrək meşəli çəmənliklərdən, enliyarpaqlı dağ meşələrindən (palıd, vələs, fıstıq), subalp və alp çəmənliklərindən ibarətdir. Heyvanat aləminə qayakeçisi, çölsiçanı, cüyür, çöldonuzu, sincab, süleysin və s. aiddirlər. Rayonun cəmi torpaq sahəsi 166488 hektardır. Ondan da 75781 hektarı kənd təsərrüfatına yararlı, 12102 hektarı isə əkin yeridir.
Qubadlı rayonunda əsasən, qəhvəyi dağ-meşə torpaqları yayılmışdır. Əsas bitki örtüyü kollu və seyrək meşəli çəmənlərdir. Dağ meşələri (fıstıq, palıd, vələs və s.) var. Meşələrin sahəsi 13,2 min hektardır. Heyvanları ayı, canavar, vaşaq, tülkü, boz dovşan, süleysin, oxlu kirpi və s-dir. Quşlardan boz kəklik, turac, qırqovul, göyərçin və s. var. Rayonda Qubadlı yasaqlığı təşkil edilib. 1 yanvar 1914-cü il tarixinə