UDC 004.056 https://doi.org/10.20535/2786-8729.4.2024.305130

COMBINED PRETTY GOOD PRIVACY AND ROLE-BASED ACCESS CONTROL MODEL FOR CONFIDENTIAL DATA PROTECTION

Danyl Kolmahin
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0009-0008-9992-3775

Anatoliy Sergiyenko
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: http://orcid.org/0000-0001-5965-1789

This article discusses a granular access protection model based on the combination of PGP (Pretty Good Privacy) and RBAC (Role-Based Access Control). The proposed model ensures an increased level of security through data encryption and role-based access control, enabling effective management of confidential data in modern information systems.

Key words: pretty good privacy, role-based access control, data encryption, information security, access management.

1. Introduction

The field of information security is critical in today's digital age, especially concerning the protection of confidential data. As organizations increasingly rely on digital systems to store and manage sensitive information, the need for robust security mechanisms becomes paramount. This article delves into the intersection of two pivotal technologies — Pretty Good Privacy (PGP) and Role-Based Access Control (RBAC) — to address the pervasive challenges in data security.

Modern information systems face numerous issues regarding the protection of data at rest, primarily concerning encryption and access management. Traditional methods often struggle to balance security and accessibility, leading to either overly restrictive access controls or inadequate protection against unauthorized access. Specifically, data encryption at rest presents significant challenges in key management and user access differentiation, which can hinder both security and operational efficiency.

This article proposes a comprehensive access protection model that combines PGP and RBAC technologies to enhance data security and provide flexible, role-based access control. The main objective is to develop a granular access control system that leverages PGP for robust data encryption and RBAC for precise access management. By integrating these technologies, the model aims to mitigate the existing problems of key management and access control, ensuring that only authorized users can access sensitive information while maintaining system usability.

The detailed discussion includes an analysis of current data encryption and access management methods, highlighting their benefits and limitations. It also explores the development and implementation of a new model that integrates PGP and RBAC, presenting a step-by-step guide on its functioning, effectiveness, and potential applications. By addressing both encryption and access control, the article contributes to the broader discourse on enhancing information security through innovative technological integration.

2. Security in confidential data processing systems

Ensuring a high level of security in systems that process confidential data is an urgent need of modern information technology. In the context of the constant increase in data volumes and the expansion of cyber threats, security becomes one of the most important aspects in the development and implementation of information systems. Despite significant progress in this area, there are a number of unresolved problems that require further investigations. One of the main problems is ensuring data encryption security at rest. Many systems still face challenges related to the effective management of encryption keys and ensuring their security [1].

The database developers propose solutions for data encryption at rest, but these solutions have their limitations. For example, database developers suggest encrypting the entire database or even encrypting the entire system (device), which increases the overall security level but does not solve the problem of convenient data access. As noted in [2], this approach provides a basic level of protection but complicates the operational work with data, especially when it is necessary to ensure flexible access to different parts of the database [3].

The research presented in [4], highlights that even after the implementation of database encryption, new problems arise. One of these problems is ensuring convenient and easy access to encrypted data. The data encryption at rest often leads to a decrease in the convenience of working with them, which, in turn, affects the performance of the system [5].

Moreover, even if a certain level of access convenience is achieved, the problem of insufficient differentiation of access between users remains. Encrypting the entire system or database does not allow flexible adjustment of access rights for different users or groups of users, which can lead to a decrease in security levels. As a result, all users who have access to the encrypted system receive the same level of access to all data, which contradicts the principles of least privilege [6].

Thus, modern approaches to data encryption at rest need improvement to ensure more flexible and secure management of access to the confidential data.

In the context of a secret management system, two important security aspects — data encryption and access control — are often considered separately. The data encryption, particularly the use of PGP, and access control using RBAC were combined into a single system that provides granular control over access and secure storage of secrets [7].

PGP is used for data encryption, ensuring the security of secrets at rest and during transmission. This method uses a hybrid approach to encryption, combining symmetric encryption for data and asymmetric encryption for key exchange. The use of public and private keys in PGP ensures that only the owners of the corresponding private keys can decrypt the data.

RBAC is used to determine who can access the system and how. This model allows system administrators to establish policies that define which user roles have access to certain resources [8].

Casbin is a powerful and flexible library for access management that supports various access control models, such as RBAC ABAC, and even more complex customizable models. The use of Casbin in the secret management system allows for a declarative approach to defining access policies, significantly improving the ability of system administrators to configure and adapt security rules according to changing requirements [9].

Casbin uses a unique approach based on models and policies. Models define the structure of security policies, indicating which factors should be considered when making access decisions, while policies define which actions are allowed or prohibited for individual users or groups. This allows the system to be dynamic and easily adaptable to new requirements, ensuring strict compliance with established access rules [10].

3. Aim and Objectives of the Study

The purpose of this article is to develop and substantiate a granular access protection model for confidential data based on the combination of PGP and RBAC technologies. The proposed model is designed to ensure a high level of security through effective data encryption and flexible role-based access management, allowing for efficient management of confidential data in modern information systems.

To achieve this goal, the following tasks are defined:

– To analyze existing methods for protecting confidential data: Review modern approaches to data encryption and access management, study their advantages and disadvantages, and identify current problems related to ensuring data security at rest.

– To develop an access protection model based on PGP and RBAC: Create a model that combines PGP and RBAC technologies to ensure a high level of protection for confidential data, considering the need for flexible access management and effective data encryption. In the framework of this project, the need for integrating these processes to ensure greater flexibility and security became apparent.

– To implement and test the model: Implement the developed model in a real information system, conduct testing to evaluate its effectiveness and ease of use.

– To evaluate the results: Analyze the obtained results, determine the level of security provided by the new model, and compare it with existing methods for protecting confidential data.

The proposed granular access protection model aims to provide not only a high level of encryption but also flexible role-based access control, which will increase the overall security and efficiency of managing confidential data in modern information systems.

4. PGP and RBAC model of access protection

4.1. The object and hypothesis of the study

The object of the study is protection of confidential data in the information security field. The systems for managing confidential data in modern information technologies are considered. The subject of the research is encryption and access control methods, particularly the combination of PGP (Pretty Good Privacy) and RBAC (Role-Based Access Control) technologies to ensure a high level of security for confidential data.

The hypothesis is that combining the methods PGP and RBAC provides more effective granular access protection in confidential data processing. The combination of PGP and RBAC technologies can be an effective solution to this problem, providing not only a high level of encryption but also flexible role-based access control.

4.2. Combined PGP and RBAC model development

Various methods are used in the research for developing and implementing the access protection model for confidential data. The main methods are:

– Literature analysis method: The analysis of modern research and publications related to data encryption and access control methods. Special attention was paid to international research and the experience of implementing similar systems in foreign companies.

– System analysis method: Study of existing systems for managing confidential data and identifying their advantages and disadvantages. The comparison of different approaches to ensuring data security at rest and during transmission.

– Modeling method: Development of a granular access protection model based on PGP-RBAC. Creation of diagrams illustrating the structure and principles of operation of the integrated system.

An extensive comparative analysis of existing secret management systems, including HashiCorp Vault, Google Cloud Secret Manager, and Sealed Secrets was performed in this research. Each system was evaluated based on key criteria such as security features, ease of integration, and flexibility in dynamic environments. The results of this analysis are summarized in Table 1, which guided the decision-making process and highlighted the need for a more robust solution.

Table 1
Comparison of existing methods of secret management

Characteristic	**HashiCorp Vault**	**Google Cloud Secret Manager**	**Sealed Secrets**
Open source	No	No	Yes
Dynamic secret management	Yes	Yes	No
Available outside the cloud	Yes	No	Yes
Vendor Lock-in	No	No	Yes
Local secret management	No	No	No (but relatively easy to implement)
Intuitive user interface	Yes	Yes	No
Audit and monitoring	Yes	Yes	No
IAM support	Yes	Yes	No
API/SDK support	Yes	Yes	No

Based on this analysis, it became clear that none of the existing tools meet all the requirements that have been set for security, flexibility and platform independence. This led to the need to develop a new approach that would combine the advantages of existing systems and eliminate their shortcomings.

The schematic diagrams in Fig. 1 and Fig. 2 illustrate the structure and principles of operation of the integrated PGP-RBAC system.

These diagrams show the key components of the system and their relations during the confidential data access algorithm execution. They include the management of encryption keys and access roles, and demonstrate how these components interact to ensure security and flexibility in managing data access.

The main principles of the model are the following.

– Data encryption with PGP: Each secret or group of secrets is encrypted using PGP symmetric keys. These encryption keys are then encrypted with the public keys of users who are allowed access to these secrets. This approach ensures that secrets can be securely stored and transmitted but are accessible only to users with the appropriate rights.

– Access control via RBAC: Access to encrypted data is controlled through roles defined in the RBAC system. Each role is associated with a specific set of privileges that determine which resources a user has access to. These roles also determine whose public keys are used to encrypt the symmetric keys that protect the data.

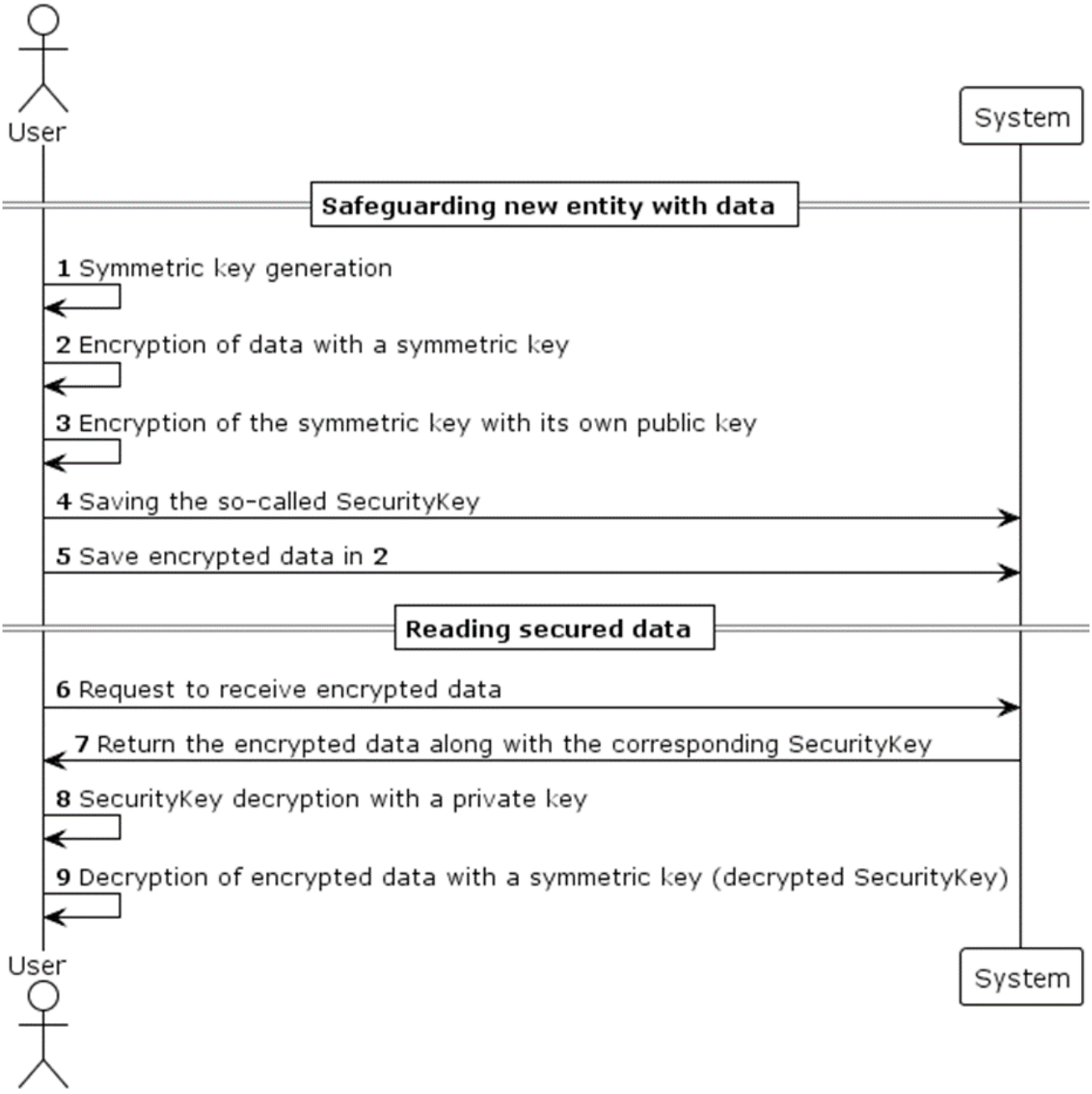

Fig. 1. PGP-RBAC granular access safeguarding model (part 1).

The model operation mechanism is the following.

– Defining roles and rules: Initially, roles and associated access rights are defined according to the organization's security policies. Each role has specific limitations regarding access to resources and operations it can perform.

– Secret initialization: When a secret is created or updated, it is encrypted with the SecurityKey of the namespace to which the secret belongs.

– Rights transfer: If one user wishes to share rights with another, the transfer occurs according to PGP with the difference that if rights are transferred to a namespace, this namespace must be accessible to the transferring party for reading according to RBAC.

– Namespace initialization: To create a secret, a namespace is first created to which this secret will belong. Along with the namespace, a symmetric key is created and stored as a "SecurityKey." The SecurityKey is associated with both the user who created the namespace (who has a pair of asymmetric keys) and the namespace itself. The main aspect stored in the SecurityKey is the asymmetric key encrypted with the appropriate user's public key, requiring PGP for its operation.

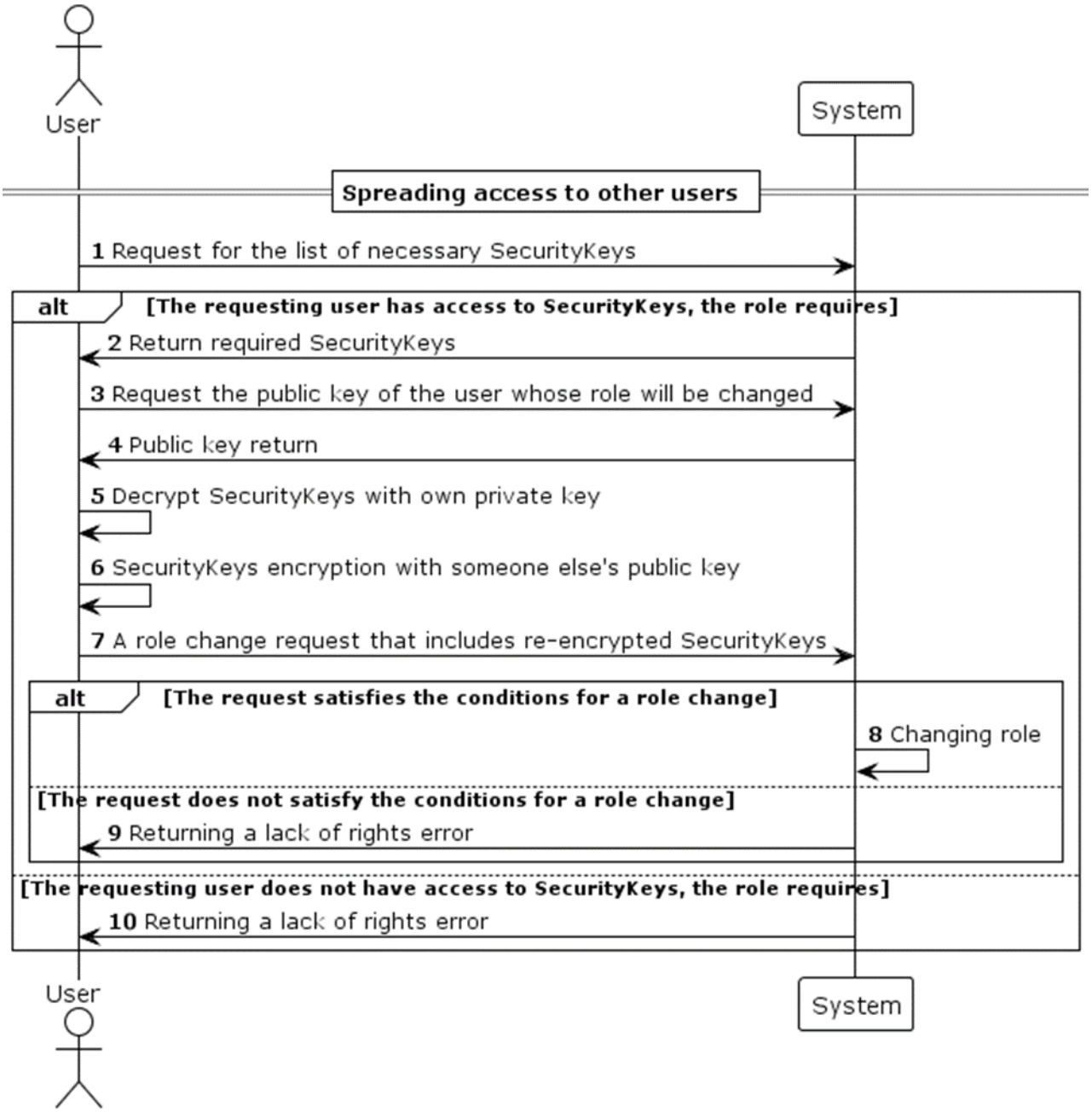

Fig. 2. PGP-RBAC granular access safeguarding model (part 2).

Thus, assuming the database is not compromised, the user access distribution is protected by verifying their privileges according to RBAC. However, even if the database is compromised, the SecurityKey still physically (i.e., privileges can be ignored, but the SecurityKey cannot) duplicates read access. Therefore, even with absolute access to the database, privileges can be bypassed, but the

SecurityKey cannot. Consequently, all accesses issued before the database compromise are protected even after this moment. This access protection model, due to the ability to divide read rights among certain user groups without creating a single user with access to all data at once, additionally increases the system's security

5. Results of investigations

The developed access protection model for confidential data based on the combination of PGP and RBAC technologies was implemented in a real information system and thoroughly tested (Fig. 3).

```
$ curl -s -o /dev/null -w "%{http_code}" 'https://ideal-octo-chainsaw.xyz/api/secrets'
\
  -H 'accept:>  application/json, text/plain, */*' \
  -H 'accept> -language: en-US,en;q=0.9,uk-UA;q=0.8,uk;q=0.7' \
>   -H 'content-type: application/json' \
  -H 'cook> ie: pvisitor=53d517f8-8e5d-4fc3-9436-eec337c231ee; SMS_ACCESS_TOKEN=eyJhbGc
iOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhYTIyNzFhMS04Nzc3LTRjODItOGI2Yy0yYWI1MDk5NmFjO
TkiLCJwcm9qZWN0SWQiOiIyMDljMTUzMy1lYjIxLTQzMTctOGQxNS1jNGI5YjllNDUzZGUiLCJlbWFpbCI6ImRl
dkBleGFtcGxlLmNvbSIsInByb2plY3ROYW1lIjoicHJvamVjdDEiLCJpYXQiOjE3MTcwMDYzMDcsImV4cCI6MTc
xNzMwNjMwN30.Ae8R2HUc-a3q4t-XV-kekyTc8M6s2aVvc3eT4uSqROs' \
  -H>  'origin: https://ideal-octo-chainsaw.xyz' \
  -H > 'priority: u=1, i' \
  -H 'referer: https://ideal-> octo-chainsaw.xyz/namespaces-secrets' \
  -H 'sec-> ch-ua: "Google Chrome";v="125", "Chromium";v="125", "Not.A/Brand";v="24"' \
  -H 'sec-ch-ua-mobile: > ?0' \
  -H 'sec-ch-ua-platform: "Windows"' \
  -H > > 'sec-fetch-dest: empty' \
  -H 'sec-fetch-mode: co> rs' \
  -H 'sec-fetch-site: same-origin' \
  -H 'u> > ser-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHT
ML, like Gecko) Chrome/125.0.0.0 Safari/537.36' \
  --data-raw '{"name":"M> Y_SECRET","encryptedValue":"alhhPhfobJsubhUTSe7CKavws2HT","na
mespaceId":"dcd421c7-4970-4de7-a5d9-ced4fe4267b6"}'
201$
```

Fig. 3. Developed system demonstrating the use of PGP-RBAC for secret preservation.

This figure is the screenshot of the console window, which shows an example of the secured data access transactions using the proposed technology.

The main evaluation criteria for the proposed model were security level, access management flexibility, system performance, and ease of use.

The key research results showed the following advantages:

– High level of security: Data encryption with PGP ensures that confidential information remains protected even in the event of a database compromise. The use of public and private keys for encrypting symmetric keys further increases the level of protection, preventing unauthorized access to data.

– Flexible access management: The use of RBAC allows system administrators to efficiently manage user access rights. Defining roles and privileges for each user ensures that only authorized individuals have access to confidential information, preventing accidental or malicious access to data.

– Improved system performance: Despite the complexity of encryption and key management, the system demonstrated high performance. Optimization of data encryption and decryption processes, as well as effective role and privilege management, ensured stable system operation without significant impact on performance.

– Ease of configuration and use: The integration of Casbin for declarative access management significantly simplified the configuration of security policies, allowing system administrators to easily adapt access rules according to changing requirements.

6. Discussion of the implemented model performance

The proposed access protection model for confidential data, based on the combination of PGP and RBAC technologies, demonstrates high efficiency in ensuring the security of modern information systems. The executed research and implementation of the developed system allows us to make the following generalized conclusions about its features:

– High level of security: Using PGP for data encryption guarantees the protection of confidential information even in the event of a database compromise. Public and private keys provide reliable encryption of symmetric keys, preventing unauthorized access to the data.

–Flexibility in access management: The RBAC model allows system administrators to effectively manage user access rights by defining roles and privileges for each user. This ensures authorized access to confidential information, minimizing the risk of accidental or malicious access.

– Improved system performance: Despite the complexity of encryption and key management processes, the system demonstrated high performance. The optimization of encryption and decryption processes, along with effective role and privilege management, ensured stable system operation without significant impact on performance.

– Ease of configuration and use: The integration of Casbin for declarative access management significantly simplified the configuration of security policies, allowing system administrators to easily adapt access rules according to changing requirements.

Further research may be aimed at expanding the functionality of the developed model. In particular, a promising direction is the use of a pair of asymmetric keys not only to ensure the impossibility of data being read by attackers but also to sign the data to prevent unnoticed changes. This approach will further enhance security by ensuring data integrity and authenticity. Implementing digital signatures will allow detecting any attempts at unauthorized data modification, significantly increasing the overall level of information system protection.

Another innovative approach is integrating blockchain technology for managing encryption keys and access logs. Blockchain can provide a tamper-proof ledger of all key management activities and access attempts, ensuring transparency and accountability. Each access request and key management operation can be recorded on the blockchain, creating an immutable audit trail that can be used to detect and prevent unauthorized activities.

The future work could explore the integration of artificial intelligence (AI) and machine learning (ML) techniques to enhance the security and efficiency of access management systems. AI and ML could be utilized to analyze access patterns, detect anomalies, and provide predictive insights to further strengthen the security posture of the system.

Conclusion

The proposed model has proven its effectiveness in ensuring a high level of security and flexible access management for confidential data. The test results showed that the model could be successfully implemented in real conditions, providing reliable data protection. Thus, the developed model is an effective solution for protecting confidential data in modern information systems and has great potential for further development and improvement. Continued innovation and integration of emerging

technologies will be essential in maintaining the robustness and effectiveness of the proposed model in the ever-evolving landscape of cybersecurity threats.

Further research is intended for expanding the functionality of the developed model.

References

[1] K. Hong, Y. Chi, L. R. Chao, and J. Tang, "An integrated system theory of information security management", *Inf. Manage. Comput. Secur.*, vol. 11, no. 5, pp. 243–248, Jan. 2003. doi: 10.1108/09685220310500153

[2] "PostgreSQL: About." PostgreSQL: The world's most advanced open source database. Accessed: May 24, 2024. [Online]. Available: https://www.postgresql.org/about

[3] D. A. Ulybyshev, "Data protection in transit and at rest with leakage detection", May 2019. doi: 10.25394/PGS.8024345.v1

[4] S. K. Basak, J. Cox, B. Reaves, and L. Williams, "A comparative study of software secrets reporting by secret detection tools", *in 2023 ACM/IEEE Int. Symp. Empirical Softw. Eng. Meas.* (ESEM). 2023, pp. 1–12. doi: 10.1109/ESEM56168.2023.10304853

[5] S. K. Basak, L. Neil, B. Reaves, and L. Williams, "What are the practices for secret management in software artifacts?", *in 2022 IEEE Secure Develop. Conf. (SecDev)*. 2022, pp. 69–76. doi: 10.1109/SecDev53368.2022.00026

[6] "Vault | HashiCorp Developer." *Vault | HashiCorp Developer*. Accessed: May 24, 2024. [Online]. Available: https://developer.hashicorp.com/vault/docs/what-is-vault

[7] S. I. S, M. N. R, and S. V. Sathyanarayana, "A comparative analysis of Secret Sharing Schemes with special reference to e-commerce applications", in *2015 Int. Conf. Emerg. Res. Electron., Comput. Sci. Technol.* (ICERECT). 2015, pp. 17–22. doi: 10.1109/ERECT.2015.7498980

[8] R. S. Sandhu, "Role-based access control" in *Advances in Computers*, Amsterdam, The Netherlands: Elsevier, vol. 46, pp. 237–286, 1998. doi: 10.1016/S0065-2458(08)60206-5

[9] Y. Luo, Q. Shen, and Z. Wu, PML: An Interpreter-Based Access Control Policy Language for Web Services. 2019. doi: 10.48550/arXiv.1903.09756

[10] R. Sandhu and P. Samarati, "Access control: Principle and practice", *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 40–48, 1994. doi: 10.1109/35.312842

УДК 004.056 https://doi.org/10.20535/2786-8729.4.2024.305130

ПОЄДНАННЯ ТЕХНОЛОГІЙ PRETTY GOOD PRIVACY ТА КОНТРОЛЮ ДОСТУПУ НА ОСНОВІ РОЛЕЙ ДЛЯ ЗАХИСТУ ДОСТУПУ ДО КОНФІДЕНЦІЙНИХ ДАНИХ

Даніл Колмагін
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: http://orcid.org/0009-0008-9992-3775

Анатолій Сергієнко
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», Київ, Україна
ORCID: http://orcid.org/0000-0001-5965-1789

У даній статті представлено гранулярну модель захисту доступу до конфіденційної інформації яка об'єднує технології PGP (Pretty Good Privacy) та RBAC (Role-Based Access Control). Метою дослідження є розробка та обґрунтування моделі що забезпечує високий рівень безпеки завдяки ефективному шифруванню даних та гнучкому управлінню доступом на основі ролей. У статті розглянуто об'єкти дослідження які включають сучасні інформаційні системи що обробляють конфіденційні дані та предмет дослідження який охоплює методи шифрування та контролю доступу.

Для досягнення поставленої мети проведено аналіз сучасних підходів до шифрування даних та управління доступом вивчено їхні переваги та недоліки а також виявлено поточні проблеми пов'язані із забезпеченням безпеки даних у стані спокою. Було розроблено модель захисту доступу що поєднує PGP і RBAC реалізовано її в реальних умовах та проведено тестування для оцінки ефективності та зручності використання. Використання PGP дозволяє забезпечити безпеку даних у стані спокою та під час передачі тоді як RBAC дозволяє гнучко налаштовувати права доступу для користувачів.

Результати досліджень показали що запропонована модель забезпечує високий рівень безпеки гнучкість управління доступом а також покращену продуктивність системи. Використання публічних та приватних ключів для шифрування симетричних ключів додатково підвищує рівень захисту запобігаючи несанкціонованому доступу до даних. Визначення ролей та привілеїв для кожного користувача забезпечує авторизований доступ до конфіденційної інформації що мінімізує ризик випадкового або зловмисного доступу до даних. Незважаючи на складність процесів шифрування та управління ключами система продемонструвала високу продуктивність оптимізовані процеси шифрування та дешифрування даних а також ефективне управління ролями та привілеями користувачів. Запропонована модель довела свою ефективність у забезпеченні високого рівня безпеки та гнучкого управління доступом до конфіденційних даних.

***Ключові слова*:** PGP, RBAC, шифрування даних, інформаційна безпека, управління доступом.