DOI: https://doi.org/10.36910/6775-2524-0560-2021-43-23
УДК 004.588
Семченко Ганна Петрівна, магістр з телекомунікацій
https://orcid.org/0000-0001-6910-9184
Одеська національна академія зв'язку ім. О. С. Попова

РОЗРОБКА МОДЕЛІ ЗАХИЩЕНОГО ІНТЕРФЕЙСУ ПЕРЕДАЧІ ДАНИХ ПРИ РОБОТІ З ХМАРНИМИ СЕРВІСАМИ

Семченко Г. П. Розробка моделі захищеного інтерфейсу передачі даних при роботі з хмарними сервісами. Розглянуто особливості організації автоматизованих систем захисту даних при застосуванні програмних додатків та інформаційних сховищ хмарних сервісів у військовій сфері. Узагальнено модель захищеного інтерфейсу взаємодії програмного додатку і апаратної платформи мережевого ресурсу, що дозволяє приховати послідовність виконання процедур зчитування та запису даних на фізичному рівні роботи з оперативною пам'яттю серверу. Зазначено, що пріоритет у розвитку сучасних схем ORAM полягає не тільки у забезпеченні надійної передачі «чутливих даних», але і в оптимізації алгоритмів їх захисту за умови збереженнявеликих обсягів даних у середовищі хмарного сервісу. Запропонована схема організації інтерфейсу на базі ORAM показує високий рівень захищеності зберігання даних на стороні сервера при прийнятному рівні захисту і ефективності виконання відповідних процедур на етапі передачі даних.
Ключові слова:хмарний сервіс, мобільні військові системи зв'язку, передача даних, збереження даних, протоколи захисту «чутливих даних», оперативна пам'ять, інтерфейс ORAM.

Семченко А. П. Разработка модели защищенного интерфейса передачи данных при работе с облачными сервисами. Рассмотрены особенности организации автоматизированных систем защиты данных при применении программных приложений и информационных хранилищ облачных сервисов в военной сфере. Построена универсальная модель защищенного интерфейса взаимодействия программного приложения и аппаратной платформы сетевого ресурса, которая позволяет скрыть последовательность выполнения процедур считывания и записи данных на физическом уровне работы с оперативной памятью сервера. Отмечено, что приоритет в развитии современных схем ORAM заключается не только в обеспечении надежной передачи «чувствительных данных», но и в оптимизации алгоритмов их защиты при сохранении больших объемов данных в среде облачного сервиса. Предложенная схема организации интерфейса на базе ORAM показывает высокий уровень защищенности хранения данных на стороне сервера при приемлемом уровне защиты и эффективности выполнения соответствующих процедур на этапе передачи данных.
Ключевые слова: облачный сервис, мобильные военные системы связи, передача данных, хранения данных, протоколы защиты «чувствительных данных», оперативная память, интерфейс ORAM.

Semchenko Hanna. Development of the secure data transfer interface model for cloud services. The peculiarities of the automated data protection systems organization when using software applications and information storages of cloud services in the military sphere are considered. There were proposed basic model of the secure interface for interaction between the software application and the network resource hardware platform allows one to hide the sequence of execution of procedures for reading and writing data at the physical level of working with the server's RAM. It is noted that the priority in the development of modern ORAM schemes is not only to ensure reliable transmission of "sensitive data", but also to optimize protection algorithms while storing large volume of data in a cloud service environment. The proposed ORAM-based interface organization scheme shows a high level of data storage security on the server side with an acceptable level of protection and efficiency of the corresponding procedures at the data transfer stage.
Keywords: cloud service, mobile military communication systems, data transmission, data storage, "sensitive data" protection protocols, random access memory, ORAM interface.

Вступ. Аналіз принципів ведення бойових дій за умов сучасного світу вказує на зростання пріоритету показника точності прийняття рішень на всіх етапах планування і контролю при організації військових операцій. Слід зазначити, що це характерно для всіх можливих задач, як то: розрахунок координат приведенні артобстрілу та проведенні бомбардування, передислокація військових частин і евакуація населення у випадку виникнення потенційної загрози, налаштування систем зв'язку, навігаційних систем, захисних комплексів, тощо. Очевидно, що у першу чергу це пов'язано з розширенням та вдосконаленням пристроїв реєстрації і збереження даних, а також інфраструктури глобальних і локальних мереж передачі даних. Інтенсивний розвиток цифрових технологій, що спостерігається протягом останніх трьох десятиріч значним чином розширив функціонал засобів ведення бою, але й,водночас, розширив коло завдань, що мають бути вирішені. Зазначена метазадача на рівні інформаційних технологій (ІТ) може формалізована якзадача роботи з великими об'ємами даних у режимі реального часу або за умов значних обмежень на час обробки вхідних запитів.

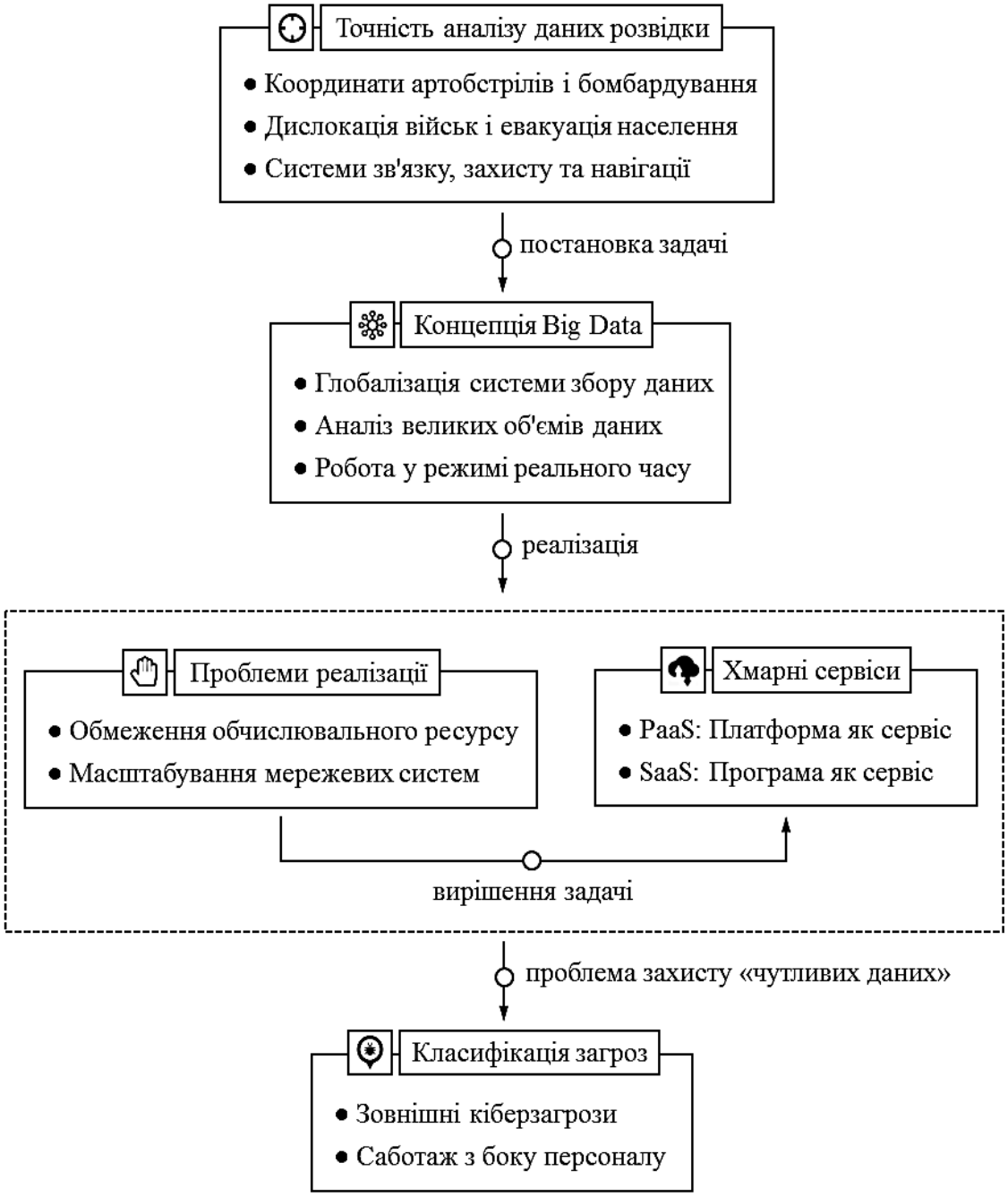

Рис. 1. Актуалізація протоколів захисту «чутливих даних» при організації військових операцій

Обмеженість обчислювального ресурсу мобільних військових частин та необхідність передачі даних від мережі інформаційних вузлів, значна частина яких також є мобільною, призводить до необхідності у застосуванні хмарних сервісів[1-3], як на рівні використання апаратної платформи (Platform as a Service, PaaS), так і на рівні застосування програмних додатків (Software as a service, SaaS). Очевидно, що відповідні дані можуть бути віднесені до «чутливих даних», що не мають бути перехоплені і використані супротивником. У той же час на для хмарних сервісів внаслідок зовнішніх атак та саботажу на внутрішньому рівні проблема організації ефективної стратегії захисту даних від перехоплення (Data Leakage Prevention, DLP) досі вважається невирішеною. І якщо у випадку з даними, що становлять комерційну цінність, збитки пов'язані з неефективністю протоколів DLP покриваються власником хмарного сервісу через юридичне вирішення конфлікту, збитки, що виникли від перехоплення даних військових є непоправними.

З метою вирішення зазначених проблем було проведено ***аналіз сучасних досліджень і публікацій*** присвячених проблемам організації військових протоколів захищеної передачі і збереження даних у середовищі хмарних сервісів. Аналіз показав пріоритет методів, що базуються на застосуванні

у зазначеній галузі інтерфейсів доступу до оперативної пам'яті типу «ORAM» (Oblivious Random Access Memory), що надають можливість застосувати протокол захисту на фізичному рівні функціонування системи [4-6].Для визначення базових підходів оптимізації ORAM-інтерфейсів відповідно до особливостей поставленого завдання були розглянуто алгоритми, що застосовуються у цивільних протоколах центрів обробки даних (ЦОД) у рамках загальної DLP-стратегії при передачі клієнтом великих об'ємів даних [7-9].Значна частина сучасних підходів реалізації DLP-протоколу на основі інтерфейсу ORAM полягає у поділенні інформаційного сховища хмарного сервісу на фіксовану кількість розділів в залежності від кількості експортованих користувачем блоків даних. Кожен з розділів працює відповідно до інтерфейсу ORAM, а алгоритм розташування блоків відповідно до карти розділів при цьому утримує лише користувач. Алгоритми «Burst ORAM» [10], «Partition ORAM» [11, 12],«Ring ORAM» [13] і «Path ORAM» [14] є типовими алгоритмами, що дозволяють оптимізувати запропонований підхід з метою зменшення затримки під час передачі даних у рамках захищеного протоколу класу ORAM.

Проведений аналіз показав високу ***актуальність*** робіт у галузі оптимізації алгоритмів організації захищених інтерфейсів класуORAM. Водночас було зазначено, що дослідницькі роботи у відповідній галузі у першу чергу спрямовані на оптимізацію процесу передачі даних, у той час як розмір інформаційного сховища, що потребується для надійного збереження даних дедалі зростає (зокрема, у рамках алгоритмів «Burst ORAM» і «Partition ORAM» хмарний сервіс виділяє інформаційне сховище, що у 3-4 рази більше за об'єм інформації, що зберігається, а у випадку більш сучасних алгоритмів «Ring ORAM» розмір сховища виростає у 6-8 разів). На сьогоднішній день вартість пов'язана зі збільшенням розміру інформаційного сховища перевищує кошти збережені за рахунок зменшення навантаження на інформаційні канали передачі даних[15-19]. Це особливо актуально для задач у рамках яких на платформі хмарного сервісу зберігаються великі об'єми даних, до яких користувач відповідного сервісу не звертається регулярно (архівні дані, актуальні дані, що протягом значного часу зберігаються на платформі користувача, тощо). Зазначені обмеження розглядаються як ***невирішена частина загального дослідження*** по застосування ORAM-інтерфейсу у військових системах мобільного зв'язку, збереження оперативних даних тапроведення хмарних обчислень.

Таким чином, ***метою роботи*** є побудова математичної моделі для розробки алгоритмів модифікації ORAM-інтерфейсу відповідно мінімізації об'ємів передачі даних та мінімізації об'ємів збереження даних при застосуванні типового для ORAM-інтерфейсу функціоналу по захисту інформації користувача.

1. Базові принципи побудови,модифікації іоцінки ефективності захищеного інтерфейсу класу ORAM

ІнтерфейсиORAM є класом захищенихінтерфейсівпередачі даних між користувачем та інформаційним сховищем хмарного сервісу, у рамках якого на фізичному рівні блокується можливість розпізнати послідовність дій користувача, тобтовиконання операцій зчитування та запису. Базова модель ORAM-інтерфейсу розглядає організацію протоколу передачі запитів від центрального процесору (Central Processing Unit, CPU) робочої станції користувача до оперативної пам'яті (Random-Access Memory, RAM) серверу хмарного сервісу, при якій послідовність операцій запису і зчитування даних неможливо відтворити на рівні інфраструктури хмарного сервісу. З іншого боку, математична модель, що розглядається у рамках даного дослідження більшою мірою відповідає сучасним підходам і формалізує процес завантаження даних з боку користувача на інформаційне сховище хмарного сервісу (процедура запису) та з інформаційного сховища хмарного сервісу на робочу станцію користувача (процедура зчитування). Формалізація полягає у визначенні набору блоків даних D_n, що може бути представлено наступним чином:

$$D_n = \{n, \{T_i^n\}, P\}, \text{де для } \forall n \in [1; N]\ i \in [1; I_n], \text{а } P = \begin{bmatrix} P_R \\ P_W \end{bmatrix}, \qquad (1)$$

де n — ідентифікатор блоку даних, $\{T_i^n\}$ — символьний набір окремого блоку даних, P — математична функція, що відповідає процедурі обробки даних, причому функція P_R відповідає процедурі зчитування, а P_W — процедурі запису даних.

Формалізація процесу роботи захищеного проколу на рівні математичної моделі може бути проведена наступним чином. Нехай множини $A: \{D_n\}$ де $n \in [1; N_A]$ та $B: \{D_n\}$, де $n \in [1; N_B]$ представляють собою послідовності операцій запису та зчитування даних користувачем у середовищі інформаційного сховища хмарного сервісу. Послідовності операцій, що виконуються з метою обробки

відповідних запитів клієнта можуть бути визначені через функції F_A і F_B, що реалізуються на рівні серверу хмарного сервісу. При цьому система контролю і моніторингу хмарного сервісу організована за принципом «Semi-Honest» (або «Honest but Curious»), тобто власник сервісу збирає і аналізує максимальний об'єм даних користувача сервісу посеред тих, що є доступними відповідно укладеної з користувачем угоди. Таким чином, достатньою умовою ефективної організації захищеногоORAM-інтерфейсу є умова еквівалентності зазначених функцій:$F_A \equiv F_B$, тобто принципова неможливість розрізнити на рівні хмарного сервісу маніпуляції користувача з блоками даних одного розміру.

2. Алгоритм оптимізації процесів використання інформаційного сховища серверу при організації ORAM-інтерфейсу

Запропонована схема оптимізації використання інформаційного сховища серверу при організації ORAM-інтерфейсу базується на застосуванні деревоподібного протоколу передачі даних[9, 11]. Це означає, що при передачі блоку даних на сервер протокол на основі випадкових функцій формує розгалужений шлях, граничні вузли (Leaf Nodes, LN) якого знаходяться у середовищі інформаційного сховища сервера. Кількість граничних вузлів, таким чином, визначає навантаження на ресурс інформаційного сховища сервера, а кількість проміжних вузлів, тобто вузлів між вузлом робочої станції клієнта (кореневим вузлом) і граничними вузлами — навантаження на ресурс перепускності інформаційного каналу. Деревоподібний протокол передачі даних у рамках ORAM-інтерфейсу характеризується надмірним навантаженням саме на ресурс інформаційного сховища [11, 14], що пропонується вирішити у рамках даного дослідження. Основними принципами оптимізації є:

- надмірність розміру граничних вузлів: збільшення розміру розділу інформаційного сховища, що виділяється для кожного граничного вузла для зменшення ймовірності його переповнення і необхідності формування додаткових граничних вузлів;
- організація m-арного дерева: збільшення арності дерева $m > 2$ замість організації двійкового дерева для зменшення розміру проміжних вузлів і шляху при великій кількості граничних вузлів.

Слід зазначити, що застосування зазначеної схеми у загальному випадку може призвести до неконтрольованого росту розміру проміжних вузлів та структури дерева шляху, що призведе до суттєвого збільшення навантаження на ресурс перепускності інформаційного каналу хмарного сервісу. З метою вирішення даної проблеми пропонується оптимізувати алгоритми запису та зчитування даних через визначення оптимального значення $m = m_{opt}$ та паралелізації і розподілення у часі операцій зчитування даних[9, 19] на базі методики DAT (De-Amortization Technique). Оптимізація має бути проведена на базі параметрів, що характеризують протокол передачі даних, зокрема:

- N — кількість реальних блоків даних (Real Blocks, RB), що передаються користувачем сервісу;
- $\bar{s} \in [1; \infty)$ — параметр, що вказує на усереднений внаслідок оптимізації розмір вузла;
- $\theta_R \in (0; 1)$ — параметр, що вказує на кількість реальних блоків даних у проміжних вузлах;
- $\theta_D \in (0; 1)$ — параметр, що вказує на кількість фіктивних блоків даних(Dummy Blocks, DB), що застосовуються у рамках протоколу захисту (символьні набори фіктивних блоків генеруються випадковим чином), у проміжних вузлах;
- $\vartheta \in (0; 1)$ — параметр, що вказує на кількість фіктивних блоків даниху проміжних вузлах.

Відповідно до цього можна визначити інформаційну ємність крайнього вузла як s_L і його частину s_L^R, що відповідає збереженню реальних блоків даних, коефіцієнт $\mu = (m-1)/2$, що визначає його межі. Визначимо математичну модель для розрахунку оптимального значення s_L^R в залежності від висоти дерева шляхуH:

$$\begin{bmatrix} 2\mu \cdot \bar{s} \le s_L^R \le \mu \cdot \bar{s} \\ s_L^R = \dfrac{s_L}{1+\vartheta} \end{bmatrix} \text{ при } H = H_0 + 1 \text{ , де } H_0 = \left\lfloor \log_m \left(\frac{N}{\mu \cdot \bar{s}} \right) \right\rfloor . \qquad (2)$$

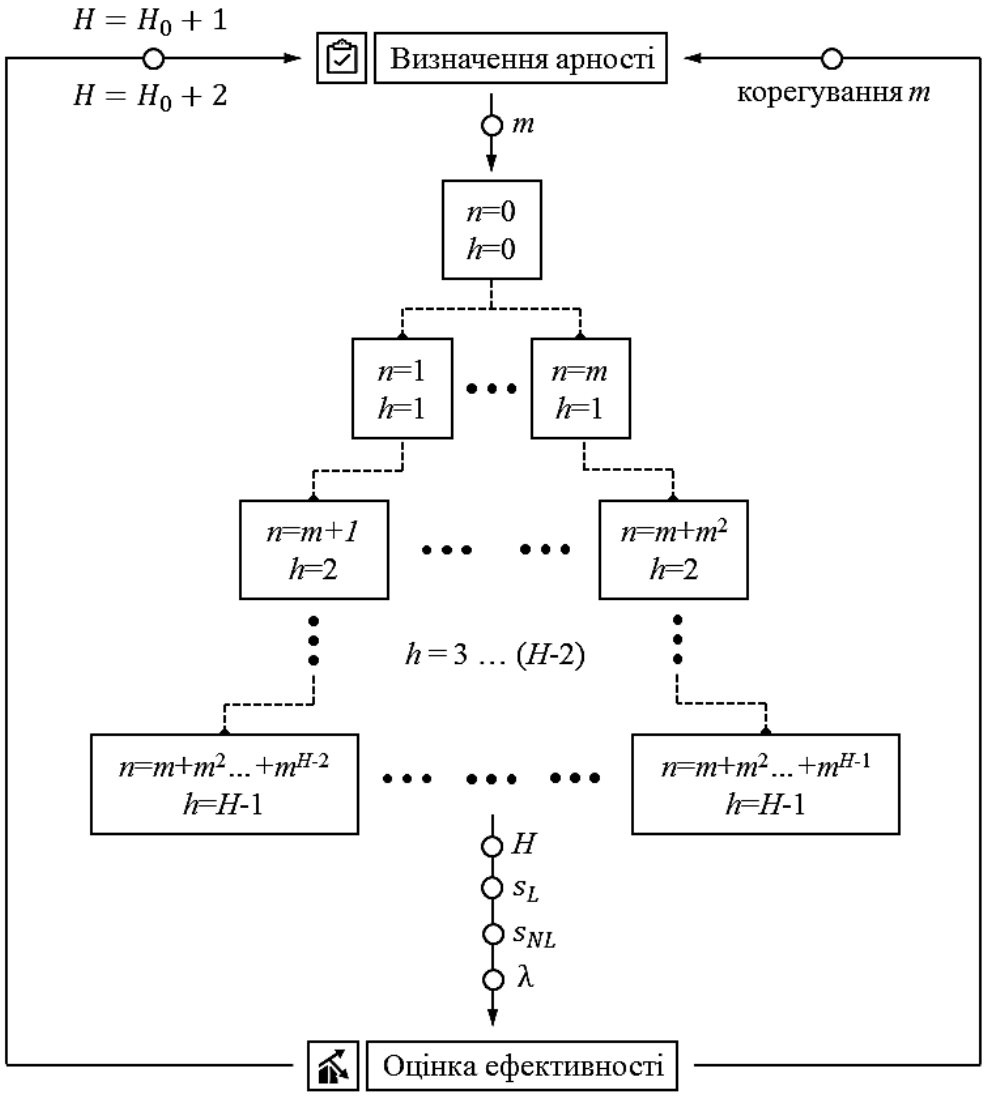

Рис. 2. Схема налаштування параметрів алгоритму організації ORAM-інтерфейсу

При $H = H_0 + 2$оптимальна залежність між значеннямиs_L і s_L^R визначаться через рівність:

$$s_L = \frac{(1+\vartheta)\cdot s_L^R}{\lfloor s_L^R/(\mu\cdot\bar{s})\rfloor}, \qquad (3)$$

і також розмір проміжних вузлів s_{NL} визначається як:

$$s_{NL} = \bar{s}\cdot\big(\mu\cdot(1+\theta_R)+(1+\theta_D)\big). \qquad (4)$$

Кожен вузол при цьому характеризується ідентифікатором $n \in [1; N]$ і рівнем $h \in [0; H-1]$,де $h = 0$ відповідає кореневому вузлу, $h \in [1; H-2]$ — проміжним вузлам, а $h = H-1$— граничним вузлам, формуючи пару $\{n, h\}$ як це показано на рис. 2.

Таким чином, налаштування алгоритму відбувається через оптимізацію шляху передачі даних через вибір арності та процедури визначення довжини шляху на основі рівня захистуORAM-інтерфейсу λ та розрахунку мінімумів H і s_{NL} , що відповідають за навантаження на ресурс перепускностіінформаційного каналу, а також s_L , що відповідає за навантаження на ресурс інформаційного сховища.

Висновки. В результаті проведеного дослідження було розглянуто принципи організації систем захисту даних при застосуванні програмних додатків та інформаційних сховищ хмарних сервісів у військовій сфері. Було узагальнено модель захищеного інтерфейсу взаємодії програмного додатку і апаратної платформи мережевого ресурсу та зазначено пріоритет схем класу ORAM.Запропоновано проводити оптимізацію дерева шляху передачі даних через вибір арності та процедури визначення довжини шляху на основі рівня захисту та розрахунку мінімумів довжини шляху і кількості проміжних вузлів, що відповідають за навантаження на ресурс перепускності інформаційного каналу, а також граничних вузлів, що відповідає навантаження на ресурс інформаційного сховища.Запропонована схема організації інтерфейсу на базі ORAM показує високий рівень захищеності зберігання даних на стороні сервера при прийнятному рівні захисту і ефективності виконання відповідних процедур на етапі передачі даних.

References.

1. Linghui, Q., &An, Z. (2015). Research on a service-oriented cloud cooperation for the new military organization. *The 27th Chinese Control and Decision Conference* (2015 CCDC). https://doi.org/10.1109/ccdc.2015.7161921.
2. Cho, S., Hwang, S., Shin, W., Kim, N., & In, H. P. (2021). Design of Military Service Framework for Enabling Migration to Military SaaS Cloud Environment. *Electronics, 10* (5), 572. https://doi.org/10.3390/electronics10050572.
3. Mauro, A. (2012). Cloud Computing: U.S. and E.U. Government/Military Approach. *Service-Oriented and Cloud Computing*, 277–278. https://doi.org/10.1007/978-3-642-33427-6_24.
4. Sasy, S., Gorbunov, S., & Fletcher, C. W. (2018). ZeroTrace : Oblivious Memory Primitives from Intel SGX. *Proceedings 2018 Network and Distributed System Security Symposium.* https://doi.org/10.14722/ndss.2018.23239.
5. Ma, Q., & Zhang, W. (2018). Towards Practical Protection of Data Access Pattern to Cloud Storage. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM).* https://doi.org/10.1109/milcom.2018. 8599798.
6. Zhang, J., Ma, Q., Zhang, W., &Qiao, D. (2017). TSKT-ORAM: A Two-Server k-ary Tree Oblivious RAM without Homomorphic Encryption. *Future Internet, 9* (4), 57. https://doi.org/10.3390/fi9040057.
7. Gentry, C., Goldman, K. A., Halevi, S., Julta, C., Raykova, M., &Wichs, D. (2013). Optimizing ORAM and Using It Efficiently for Secure Computation. *Privacy Enhancing Technologies*, 1–18. https://doi.org/10.1007/978-3-642-39077-7_1.
8. Hoang, T., Yavuz, A. A., & Guajardo, J. (2020). A Multi-server ORAM Framework with Constant Client Bandwidth Blowup. *ACM Transactions on Privacy and Security*, *23*(1), 1–35. https://doi.org/10.1145/3369108.
9. Shi, E., Chan, T.-H., Stefanov, E., & Li, M. (2011). Oblivious RAM with O((logN)3) Worst-Case Cost. *Lecture Notes in Computer Science*, 197–214. https://doi.org/10.1007/978-3-642-25385-0_11.
10. J. Dautrich and E. Stefanov. (2014) Burst ORAM: Minimizing ORAM Response Times for Bursty Access Patterns. *InProc. 23rd USENIX Security Symposium, 2014.*
11. E. Stefanov, E. Shi, and D. Song. (2011) Towards practical oblivious RAM. *In Proc. NDSS, 2011*.
12. Zhang, J., Zhang, W., &Qiao, D. (2015). GP-ORAM: A Generalized Partition ORAM. *Network and System Security*, 268–282. https://doi.org/10.1007/978-3-319-25645-0_18.
13. L. Ren, C. W. Fletchery, A. Kwony, E. Stefanov, E. Shi, M. van Dijkz, and S. Devadasy (2014) Ring ORAM: Closing the Gap Between Small and Large Client Storage Oblivious RAM. *In Proc. IACR Cryptology ePrint Archive 2014*: 997.
14. Stefanov, E., van Dijk, M., Shi, E., Fletcher, C., Ren, L., Yu, X., &Devadas, S. (2013). Path ORAM. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*. https://doi.org/10.1145/ 2508859.2516660.
15. Wang, R., Zhang, Y., & Yang, J. (2018). D-ORAM: Path-ORAM Delegation for Low Execution Interference on Cloud Servers with Untrusted Memory. *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA).* https://doi.org/10.1109/hpca.2018.00043.
16. M. T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia (2011) Oblivious RAM simulation with efficient worst-case access overhead. *In Proc. CCSW, 2011*.
17. Q. MA and W. Zhang. (2018) *Towards practical protection of data access pattern to cloud storage.* In http://www.cs.iastate.edu/wzhang/milcom18full. pdf.
18. X. Wang, T.-H. H. Chan, and E. Shi. (2015) Circuit ORAM: On tightness of the Goldreich-Ostrovsky lower bound. In Proc. *CCS, 2015*.
19. Ma, Q., & Zhang, W. (2018). Towards Practical Protection of Data Access Pattern to Cloud Storage. *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM).* https://doi.org/10.1109/milcom.2018. 8599798.