

**MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII
MOLDOVA**

Universitatea Tehnică a Moldovei

Facultate de Calculatoare Informatică și Microelectronică

Departament Ingineria Software și Automatică

Admis la susținere

Șef departament:

conf. univ., dr. Ion Fiodorov

”_____” _____ 2024

**CONTROLUL ACCESULUI BAZAT PE ATRIBUTE ȘI
POLITICI PENTRU UN SISTEM INFORMATIC DE
MARKETING**

Teză de master

Student:

Postu Ivan, SI-221M

Conducător:

**Zgureanu Aureliu,
dr. conf. univ.**

Recenzent:

**Bulai Rodica,
asist. univ.**

Chișinău, 2024

ADNOTARE

La teza de master – Controlul accesului bazat pe atribute și politici pentru un sistem informatic de marketing, elaborată de Postu Ivan, Chișinău, 2023

Cuvinte cheie: platformă de marketing, controlul accesului, sistem de autorizare bazat pe atribute și politici, program de marketing, restricționarea accesului pe bază de comportament, analiza activității utilizatorului, managementul politicilor și atributelor, atribute dinamice, integrare.

La teza lucrării de master ca scop de bază s-a pus proiectarea, modelarea și implementarea sistemului de control a accesului bazat pe atribute și politici, ca parte componentă din platformă de marketing ce oferă posibilități clienților de a promova produsul sau serviciul oferit pentru utilizatori. Pe parcursul elaborării lucrării s-a pus accent pe analiza soluțiilor existente cât în general, atât și pentru sisteme informatice din diverse domenii inclusiv și marketing. Au fost definite un set de cerințe și criterii față de modulul implementat ce ține de limitări la nivel software și anume, volum de date procesat, posibilitatea de integrare cât cu platforma de marketing existentă, atât și cu platformele clienților, flexibilitatea definirii atributelor și politicilor, mod convenabil de configurare a regulilor de acces cu absența necesității de a interveni cu modificări în logica business în mod direct. Asemenea au fost puse la bază obiectivele a acestui proiect, și anume îmbunătățirea securității datelor ce ține de programele de marketing prin implementarea unor controale fiabile și deterministe de acces, acest lucru poate preveni intruziunea neautorizată la datele sensibile din cadrul programului de marketing care sunt esențiale pentru protejarea intereselor comerciale și a confidențialității clienților. La fel unul din obiectivele principale a fost dezvoltarea controlului ce poate fi gestionat în mod dinamic prin intermediul expresiilor ce pot fi evaluate și rezultatul cărora poate fi utilizat de motorul pe baza cărui rulează programul sau setul de programe de marketing active. Acest model permite de a defini cine poate accesa ce informații în cadrul acestor programe, faptul dat a implicat definirea și controlul accesului pe baza diferitelor atribute, cum ar fi rolurile utilizatorului, locația sau datele anumitor activități din cadrul platformei clientului, toate aceste atribute fiind dinamice din motiv că platformă de marketing este una dar clienți și ariile de activitate sunt diferite. În general, obiectivele lucrării date sunt de a dezvolta un astfel sistem, ce oferă funcționalități flexibile de control a accesului pentru utilizatorii ce participă în programele de marketing definite de clienți ca parte componentă a platformei de marketing.

Tehnologii utilizate: Java17, node-js, materialize-css, MySQL, NixShell, Nix package manager, linux, bash, docker, docker-compose, react native

ANNOTATION

In the master's thesis – Access control based on attributes and policies for a marketing information system

developed by Postu Ivan, Chişinău, 2023

Keywords: marketing platform, access control, attribute and policy-based authorization system, marketing program, behavior-based access restriction, user activity analysis, policy and attribute management, dynamic attributes, integration.

The main goal of the master's thesis was to design, model and implement the access control system based on attributes and policies, as a component of the marketing platform that offers purchasing possibilities to promote the product or service offered to users. On these elaborations, emphasis was placed on the analysis of existing solutions in general, as well as for IT systems in various fields, including marketing. A set of requirements and criteria have been defined regarding the implemented mode related to software limitations, namely, volume of data processed, possibilities of integration of existing marketing platforms, as well as with customer platforms, flexibility of defining attributes and policies, mode convenient configuration of access rules with the absence of the need to intervene with changes in direct business logic. They were also based on the objective of this project, which is to create the security of data sensitive to the marketing program by implementing reliable and deterministic access controls, this can prevent unauthorized intrusion of sensitive data within the marketing program that is essential to protect the interests commercial and customer privacy. As one of the main goals was to develop control that could be dynamically managed through expressions that could be evaluated and the output of which could be used by the skill-based engine to run the active marketing program or set of programs. This model allows defining who can access information within these programs, which means that it involved defining and controlling access based on various attributes, such as user roles, location, or certain specific activities within the client's platform, all of which are dynamics. for the reason that the marketing platform is one but the areas of activity are also different. In general, the objectives of the given work are to develop such a system, which offers flexible access control functionalities for users participating in the marketing programs defined as a component of the marketing platform.

Technologies used: Java17, node-js, materialize-css, MySQL, NixShell, Nix package manager, linux, bash, docker, docker-compose, react native

Cuprins

INTRODUCERE.....	8
1 CERCETAREA ȘI ANALIZA DOMENIULUI DE CONTROL A ACCESULUI ÎN CADRUL UNUI SISTEM INFORMATIC DE MARKETING.....	9
1.1 Analiza modelului de control a accesului.....	11
1.2 Analiza soluțiilor informatice existente de control a accesului bazate pe politici, atribute și roluri.	17
1.3 Analiza comparativă a soluțiilor informatice existente de control a accesului bazate pe politici, atribute și roluri.....	21
2 PROIECTAREA ȘI MODELAREA MODULULUI DE CONTROL A ACCESULUI.....	22
2.1 Modelarea funcțională.....	23
2.2 Modelarea cazurilor de utilizare.....	27
2.3 Modelarea fluxului de control.....	32
2.4 Modelarea principiului de funcționare și integrare cu platforme externe.....	35
3. REALIZAREA SISTEMULUI.....	40
3.1. Implementarea controlului de acces bazat pe atribute și politici pentru un sistem informatic de marketing.....	40
3.2. Implementarea platformei de marketing.....	42
4. EVALUAREA PROIECTULUI.....	57
4.1. Rezultatele proiectului.....	57
4.2. Testarea sistemului.....	61
4.3. Estimarea costurilor.....	64
4.4. Analiza riscurilor.....	66
CONCLUZII.....	68
BIBLIOGRAFIE.....	70
ANEXA A – Analiza soluțiilor existente – OpenAM dezvoltat de ForgeRock.....	71
ANEXA B – Analiza soluțiilor existente – Oracle Identity and Access Management (Oracle IAM).	73
ANEXA C – Analiza soluțiilor existente – Auth0.....	74
ANEXA D – Definiere a ramurii în cadrul programului de marketing.....	75
ANEXA E – Expresii ce aparțin unei ramuri a programului de marketing.....	76
ANEXA F – Exemplu de integrare la „Platformă de asigurări medicale online”	78

INTRODUCERE

Procesul de definire a nivelului de acces pentru utilizatori la diverse resurse și informații din cadrul întreprinderii de-a lungul timpului a avut un rol major în procesul de management a riscurilor. Ignorarea acestui fapt poate afecta extrem, în mod negativ activitatea întreprinderii, chiar în unele cazuri poate contribui la falimentarea ei. În sisteme și platforme de tip business to business ce oferă clientului posibilitate de a crea programe informatice de marketing cu posibilitate de a le integra cu platforma sa, prezența unui astfel sub-sistem ce ar permite în mod flexibil și fiabil definirea regulilor și a atributelor care indică ce utilizatori, în ce circumstanțe au acces la ce categorii de resurse și în ce măsură este obligatorie. Obiectivul de bază a acestui proiect este de a oferi o soluție pentru un astfel sistem de marketing. Diferența de sistemele de autentificare și autorizare standarde este ignoranța factorilor și condițiilor specifice, sistemele standarde sunt orientate larg, în timp ce în sisteme de marketing nivelul de acces se poate baza pe diferite circumstanțe și date ce pot fi prezente în urma activității utilizatorilor sau datelor oferite de clienți în cadrul programului de marketing, de exemplu încărcate manual sau accesate prin intermediul cererilor http sau RPC în cazul în care aceste date se păstrează pe partea platformei clientului sau stocarea și utilizarea lor în logică direct de compania de marketing. Pentru lucrarea dată ca scop sa pus implementarea unui subsistem ce urmează modelul ABAC (Attribute Based Access Control) care utilizează attribute ca rolurile utilizatorului, locația sau timpul de acces pentru a lua decizii de autorizare. Obiectivul este de a crea un sistem care se adaptează la condițiile în schimbare și la contextele utilizatorilor. Un alt aspect ce subsistemul dezvoltat este necesar să suporte este managementul politicilor care permite administrarea, definirea și modificarea cu ușurință a regulilor de acces. Asemenea ca obiectiv a implementării pe partea sistemului informatic s-a pus dezvoltarea mecanismelor de audit pentru a urmări activitățile de acces și pentru a asigura conformitatea cu reglementările privind protecția datelor. Acest obiectiv se concentrează pe crearea unei evidențe solide despre cine a accesat ce date sau ce resurse și în ce moment al timpului. Una din restricțiile de bază a soluției soft dezvoltate este echilibrarea securității cu gradul de utilizare, și asigurarea că utilizatorii autorizați pot accesa eficient informațiile de care au nevoie, fără obstacole inutile. Obiectivul de bază în cazul dat fiind absența limitărilor în activitatea utilizatorilor, pentru a atinge scopul dat se va lua în calcul factorul de scalabilitate, soluția de control al accesului este necesar să se adapteze la creșterea sistemului de informații de marketing. Aceasta implică proiectarea unui sistem care poate gestiona un număr mare de utilizatori, și solicitări de acces. În general, obiectivele dezvoltării unui sistem de control a accesului bazat pe attribute și politici pentru un sistem informatic de marketing sunt de a consolida securitatea datelor, de a oferi un control flexibil și dinamic al accesului, de a asigura conformitatea și de a îmbunătăți funcționalitatea generală și capacitatea de utilizare a sistemului, menținând în același timp eficiența costurilor.

BIBLIOGRAFIE

1. M. Lehto and P. Neittaanmäki, Eds., *Cyber Security: Analytics, Technology and Automation*, vol. 78. in *Intelligent Systems, Control and Automation: Science and Engineering*, vol. 78. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-18302-2.
2. G. K. Kostopoulos, *Cyberspace and cybersecurity*. Boca Raton, FL: CRC Press, 2013. ISBN: 1466501332.
3. D. A. Chappell and T. Jewell, *Java Web services: using Java in service-oriented architectures*, 1. ed. Beijing Köln: O'Reilly, 2002. ISBN 10: 0596002696.
4. D. Resende, *Node.js high performance: take your application to the next level of high performance using the extensive capabilities of Node.js*. Birmingham, UK: Packt Publishing, 2015. ISBN: 9781785286148.
5. A. I. Awad, A. E. Hassanien, and K. Baba, Eds., *Advances in Security of Information and Communication Networks: First International Conference, SecNet 2013, Cairo, Egypt, September 3-5, 2013. Proceedings*, vol. 381. in *Communications in Computer and Information Science*, vol. 381. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. doi: 10.1007/978-3-642-40597-6.
6. J. Jacobs and B. Rudis, *Data-driven security: analysis, visualization, and dashboards*. Indianapolis, IN: Wiley, 2014. ISBN: 9781118793664.
7. A. Mitra, *Digital security: cyber terror and cyber security*. New York: Chelsea House, 2010. ISBN: 0816067910.
8. M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*. Berkeley, CA: Apress, 2019. doi: 10.1007/978-1-4842-4294-0.
9. E. Maiwald, *Network security: a beginner's guide*, 3rd ed. New York: McGraw-Hill, 2013. ISBN: 9780071795708.
10. N. Adams and N. Heard, *Data analysis for network cyber-security*. London: Imperial college press, 2014. ISBN: 978-1-783-26374-5 .
11. A. Osmani, *Learning JavaScript design patterns*, 1st ed. Sebastopol, CA: O'Reilly Media, 2012. ISBN-13. 978-1449331818.
12. C. Johansen, *Test-driven JavaScript development*. in *Developer's library series*. Upper Saddle River, NJ: Addison-Wesley, 2011. ISBN: 9780321683915.
13. M. D. Hansen, *SOA using Java Web Services*, 3. print. Upper Saddle River, NJ: Prentice Hall, 2008. ISBN: 978-13-239405-5.
14. J. Graba, *An Introduction to Network Programming with Java: Java 7 Compatible*. London: Springer London, 2013. doi: 10.1007/978-1-4471-5254-5.