**ROMÂNIA**

**MINISTERUL APĂRĂRII NAȚIONALE**

**ACADEMIA TEHNICĂ MILITARĂ ,,FERDINAND I”**

**FACULTATEA DE SISTEME INFORMATICE ȘI SECURITATE CIBERNETICĂ**

**Specializare: Calculatoare și Sisteme Informatice pentru Apărare și Securitate Națională**



**SOLUŢIE DE SECURIZARE A SERVICIILOR INTEGRATE ŞI ANONIMIZAREA ACCESULUI LA INFRASTRUCTURI VIRTUALIZATE**

CONDUCĂTOR ȘTIINȚIFIC:

**Col. prof. univ. dr. ing. Mihai TOGAN**

ABSOLVENT:

**Student plt. Ionuţ-Alexandru PAVEL**

Conţine \_\_\_\_\_\_\_\_\_\_\_ file

Inventariat sub nr. \_\_\_\_\_\_

Poziţia din indicator: \_\_\_\_

Termen de păstrare: \_\_\_\_\_

**BUCUREŞTI**

**2022**

# ABSTRACT

Collaboration tools involve multiple types of software or services that allow people to work toghether. Collaboration tools can route work through a process, distribute pieces and tasks to involved parties, and help to coordinate activities.

This paper presents the implementation of the web-based collaborative real-time application using ReactJs and NodeJs frameworks. The application provides a secure, controlled environment for real-time document review, coauthoring and redaction. Also, it allows the creation of private or group conversation beetween users and allows text message transfer. Documents can be saved in encrypted format using server storage and personal data is stored using MySql relational database. The application also ensures communication between users by creating private or public chat channels. Communication between users is secure and allows the exchange of text messages or the transmission of media files. Another communication method provided by the application is video calling, allowing users to interact directly with each other. The software solution also provides the functionality for users with an admin role to monitor the activity of other users and restrict their access to the application.

The final goal of the project is the development and operationalization of the presented software solution based on the studied concepts. An important aspect to take into account is that the application at the moment is not a final product to be put into use, but it is a demo version that puts the theoretical concepts into practice.

# REZUMAT

Cuprins

[ABSTRACT 5](#_Toc106039809)

[REZUMAT 6](#_Toc106039810)

[LISTĂ DE ABREVIERI 9](#_Toc106039811)

[TABELĂ FIGURI 9](#_Toc106039812)

[1. Introducere 11](#_Toc106039813)

[1.1 Importanţa temei 11](#_Toc106039814)

[1.2 Scopul lucrării 11](#_Toc106039815)

[1.3 Utilitatea sistemului 11](#_Toc106039816)

[2 Stadiul actual 12](#_Toc106039817)

[2.1 Software colaborativ 12](#_Toc106039818)

[2.2 Sisteme similare 12](#_Toc106039819)

[2.2.1 Microsoft Teams 12](#_Toc106039820)

[2.2.2 Slack 13](#_Toc106039821)

[2.2.3 Discord 14](#_Toc106039822)

[2.2.4 Telegram 15](#_Toc106039823)

[2.2.5 Google Docs 16](#_Toc106039824)

[2.3 Dezvoltarea aplicaţiilor web 16](#_Toc106039825)

[2.4 Tehnologii folosite în dezvoltarea aplicaţiilor de tip colaborativ?? 16](#_Toc106039826)

[3 API-uri folosite 16](#_Toc106039827)

[3.1 React 16](#_Toc106039828)

[3.2 NodeJS 16](#_Toc106039829)

[3.3 MySQL 16](#_Toc106039830)

[3.4 Socket.Io 16](#_Toc106039831)

[3.5 Axios 16](#_Toc106039832)

[4 Structura proiectului 17](#_Toc106039833)

[4.1 Cerinţele sistemului 17](#_Toc106039834)

[4.1.1 Cerinţe funcţionale 17](#_Toc106039835)

[4.1.2 Cerinţe non-funcţionale 17](#_Toc106039836)

[4.2 Arhitectura sistemului 17](#_Toc106039837)

[4.2.1 Modulele funcţionale ale sistemului 17](#_Toc106039838)

[4.2.2 Arhitectura aplicaţiei client 17](#_Toc106039839)

[4.2.3 Arhitectura aplicaţiei server 17](#_Toc106039840)

[4.2.4 Persistenţa datelor 17](#_Toc106039841)

[5 Implementarea software 17](#_Toc106039842)

[5.1 Aplicaţia client 17](#_Toc106039843)

[5.2 Aplicaţia web server 17](#_Toc106039844)

[5.2.1 Răspunderea request-urilor 17](#_Toc106039845)

[5.3 Implementarea bazei de date 17](#_Toc106039846)

[5.3.1 Diagramă 17](#_Toc106039847)

[5.4 Metode de securizare 17](#_Toc106039848)

[5.4.1 Securizarea canalului de comunicaţie 17](#_Toc106039849)

[5.4.2 Criptarea fişierelor stocate 17](#_Toc106039850)

[5.4.3 Protecţie împotriva atacurilor CSRF 17](#_Toc106039851)

[5.4.4 Controlul accesului prin firewall 17](#_Toc106039852)

[5.4.5 Alertare în cazul încercărilor neautorizate 17](#_Toc106039853)

[6 Utilizarea aplicaţiei 18](#_Toc106039854)

[6.1 Actorii sistemului 18](#_Toc106039855)

[6.2 Cazurile de utilizare 18](#_Toc106039856)

[6.3 Testarea sistemului 18](#_Toc106039857)

[6.4 Raport de testare 18](#_Toc106039858)

[6.5 Diagrame UML 18](#_Toc106039859)

[6.5.1 Diagrama cazurilor de utilizare 18](#_Toc106039860)

[6.5.2 Diagrama de activităţi 18](#_Toc106039861)

[7 Concluzii 18](#_Toc106039862)

[7.1 Analizarea rezultatelor obţinute 18](#_Toc106039863)

[7.2 Dezvoltări ulterioare 18](#_Toc106039864)

[8 Bibliografie 18](#_Toc106039865)

[9 Anexe 19](#_Toc106039866)

# LISTĂ DE ABREVIERI

|  |  |  |
| --- | --- | --- |
|  | WebRTC | Web Real-Time-Comunication |
|  | VoIP | Voice over Internet Protocol |
|  | AES | Advanced Encryption Standard |
|  | MitM | Man-in-the-Midle |
|  | ALTS | Application Layer Transport Security |
|  | TLS | Transport Layer Security |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# TABELĂ FIGURI

# 1. Introducere

## Importanţa temei

Progresul tehnologic şi necesitatea diminuării timpul de muncă împreună cu nevoia oameniilor de a menţine comunicaţia la distanţă au dus la dezvoltarea de aplicaţii software colaborative care să satisfacă aceste cerinţe într-o manieră uşor de gestionat pentru utilizator. Astfel aplicaţiile colaborative sunt dezvoltate cu scopul de a ajuta persoanele implicate în proiecte comune să îşi atingă obiectivele minimizând resursele necesare de spaţiu şi timp. Toate aceste acţiuni trebuie să fie desfăşurate într-un mediu care oferă siguranţă atât pentru utilizator, cât şi pentru pentru datele care sunt prelucrate.

## Scopul lucrării

Prezenta lucrare are ca obiectiv detalierea şi formarea cunoştiinţelor necesare pentru dezvoltarea şi operaţionalizarea unei soluţii software „on-premise” (implementată folosind resurse proprii) care să asigure activitatea colaborativă la nivelul unei organizaţii guvernamentale. Lucrarea va cuprinde informaţii despre realizarea arhitecturii aplicaţiei software, detalii despre tehnologiile folosite, informaţii despre mecanismele de securizare folosite şi parcursul instalării pe o infrastructură virtualizată proprie. De asemenea, în proiect vor fi prezentate cazurile de utilizare şi se va întocmi un raport de testare.

## Utilitatea sistemului

Organizaţiile guvernamentale lucrează cu date clasificate, care nu pot fi prelucrate folosind soluţii software externe din raţiuni de securitate. În acelaşi timp există riscul ca o aplicaţie pusă la dispoziţie de un dezvoltator extern să colecteze date cu privire la utilizator, precum locaţia acestuia, adresa IP sau activitatea acestuia la nivelul dispozitivului pe care este folosită. Astfel, apare necesitatea unei soluţii dezvoltate şi administrate de organizaţia în cauză, pentru a reduce riscul colectării şi interceptării datelor.

În acelaşi timp folosirea unei aplicaţii realizate în mediul intern oferă control absolut asupra fluxului de date (datele sunt stocate intern), dar şi asupra utilizatorilor, în cazul în care este detectată activitate suspectă poate fi restricţionat accesul la resursele interne. Regulile pe care le respectă organizaţiile guvernamentale nu permit folosirea de resurse Cloud externe pentru stocarea informaţiilor, deoarece furnizorii de servicii Cloud nu pot dovedi integritatea datelor pe care le administrează, dar şi din raţiuni politico-geografice. Soluţia propusă va îndeplinii criteriile de securitate specifice organizaţiilor guvernamentale, punând accent pe securizarea canalului de comunicaţie, stocarea datelor, dar şi monitorizării activităţii utilizatorilor.

# Stadiul actual

## Software colaborativ

Aplicaţiile software colaborative sunt concepute cu scopul de a optimiza munca în echipă prin accesarea unui mediu de lucru comun unde angajaţii pot împărtăşi cunoştinţe, date şi documente pentru a rezolva probleme specifice. Printre funcţionalităţile cel mai des puse la dispoziţie de aplicaţiile colaborative se numără: comunicaţia dintre utilizatori folosind canale de mesagerie instantă, managementul documentelor, împărţirea de sarcini, portabilitatea pe diferite tipuri de device-uri şi măsurile de securitate [1].

Lucrarea de faţă îşi propune crearea unei aplicaţii colaborative cu interfaţă web de tip „on premise”care să îndeplinească funcţionalităţi de comunicaţie şi de editare text în timp real, folosind doar servicii implementate intern. Spre deosebire de alte aplicaţii puse la dispoziţie pe piaţă, soluţia software propusă va oferi acces nelimitat despre modul de funcţionare, întrucât este implementată folosind resurse proprii, iar clientul va avea acces şi la codul sursă al acesteia. Marea majoritate a aplicaţiilor cu scop colaborativ oferite de dezvoltatori externi nu oferă servicii „on-premise”, datele clienţilor fiind administrate de dezvoltatorii în cauză.

## Sisteme similare

În momentul actual există o diversitate destul de mare de aplicaţii care oferă suport pentru munca colaborativă, cele mai multe dintre ele fiind implementate folosind Cloud extern. Acest aspect devine un criteriu important de selecţie atunci când organizaţia îşi doreşte o securitate ridicată şi lucrează cu informaţii clasificate care nu trebuie să părăsească mediul intern al organizaţiei. Printre aplicaţiile colaborative des întâlnite amintim: Microsoft Teams, Slack, Discord, Asana şi Google Docs.

### Microsoft Teams

Microsoft Teams este o aplicaţie colaborativă lansată la finalul anului 2016 care înglobează toate servicile de comunicaţie (mesagerie instantă, apeluri video şi audio, gestionare de documente), oferind suport ca aplicaţie web, aplicaţie mobilă şi aplicaţie desktop. Acest utilitar se integrează cu suita de servicii Microsoft 365 şi alte servicii furnizate de Microsoft (spaţiul de stocare Cloud)[2].

Principalele avantaje ale aplicaţiei Microsoft Teams sunt portabilitatea între dispozitive, capabilitatea de a gestiona grupuri cu un număr ridicat de utilizatori şi diversitatea serviciilor puse la dispoziţie. Acest serviciu este destinat în principal companiilor sau organizaţiilor cu un număr ridicat de utilizatori, pornind de la abonamente gratuite, până la abonamente contra cost în funcţie de necesităţile şi activitatea organizaţiei. Popularitatea de care se bucură serviciul Teams este dată de suportul şi sustenabilitatea oferite de firma Microsoft, acesta ocupând marea parte a spaţiului educaţional şi antreprenorial

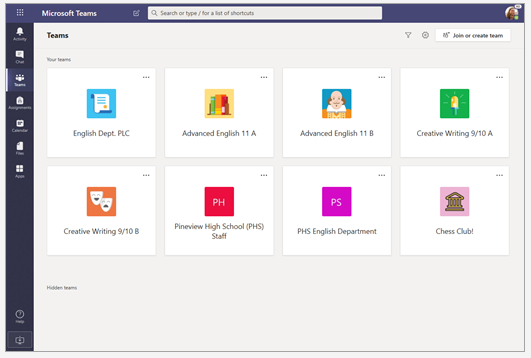


Fig. 1 - Microsoft Teams (Versiunea Desktop) – HomePage [3]

### Slack

Slack este un serviciu software de mesagerie instantanee lansat în anul 2013 şi conceput special pentru mediul de lucru din cadrul organizaţiilor. Potrivit deţinătorului companiei, numele aplicaţiei este un acronim pentru „Searchable Log of All Conversation and Knowledge”, astfel dezvăluind principala caracteristică a produsului, aceea ca toate conversaţiile şi fişierele partajate să poată fi căutate mai uşor faţă de alte dispozitive colaborative[4]. Un alt avantaj major al acestei platforme este că elimină nevoia conversaţiilor bazate pe email la nivelul organizaţiei.

Slack oferă versiuni ale aplicaţiei compatibile desktop şi mobile, dar şi o versiune de browser. Din punct de vedere al scalabilităţii, aplicaţia se remarcă prin faptul ca nu are o limită superioară al numărului de conversaţii deschise, faţă de competitorul său Teams care are o limită superioară de maxim 200 de canale la nivelul unei echipe.

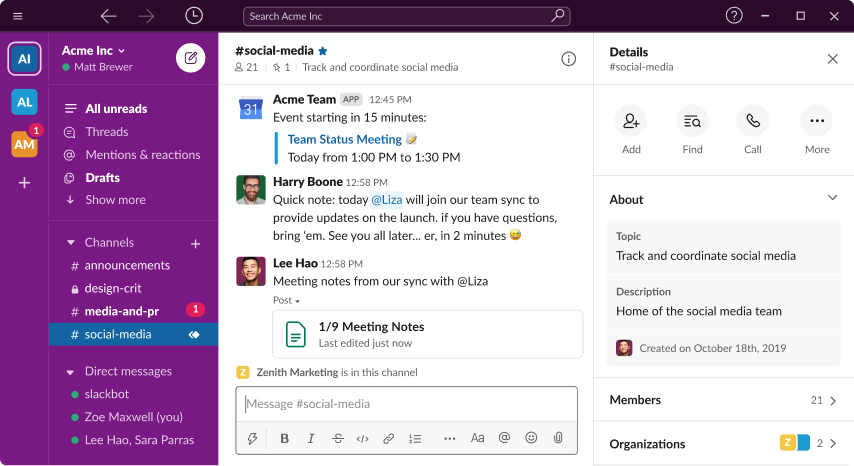


Fig. 2 – Slack (Versiunea Desktop) – HomePage [5]

### Discord

Discord este o aplicaţie cross-platform gratuită de mesagerie text, voce şi video folosită cel mai mult în scop recreativ. Popularitatea aplicaţiei este dată de faptul că este gratuită, iar limita maximă a utilizatorilor dintr-un grup poate ajunge până la 250.000, cu menţiunea că acest număr poate fi mărit. Limita de participanţi pentru un apel video este de 25 de utilizatori, iar pentru o conversaţie audio este de până la 122 de participanţi. Pentru asigurarea comunicaţiei, Discord, foloseşte tehnologia WebRTC oferită la nivelul browser-ului. Tehnologia WebRTC este disponibilă în toate browserele moderne. Pentru versiunile aplicaţiei care rulează pe alte dispozitive (desktop, mobile) este utilizat un modul media dezvoltat în C++ programat pe baza bibliotecii native WebRTC. Datorită acestui aspect unele caracteristici ale serviciului funcţionează mult mai bine pe aplicaţiile instalate decât în aplicaţia de tip browser.

Unul din dezavantajele aplicaţiei aplicaţiei sunt problemele de securitate şi incidentele petrecute în trecut precum cele de tipul phishing şi ransomware. De asemenea, aplicaţia nu eforă un serviciu de criptare end-to-end precum alte aplicaţii de chat.

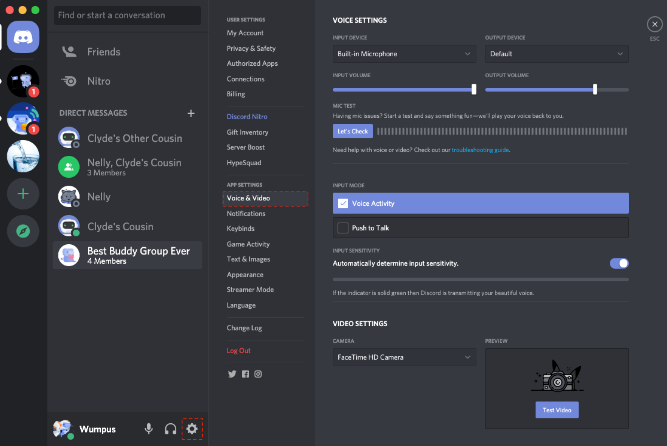


Fig. 3 – Discord (Versiunea Desktop) - Homepage[6]

### Telegram

Spre deosebire de celelalte aplicaţii prezentate până acum, Telegram este o aplicaţie colaborativă de tip open source ce prestează servicii de mesagerie text şi VoIP. Aplicaţia se remarcă prin numărul foarte mare de participanţi ce pot face parte dintr-un grup la un moment dat, în momentul de faţă acesta fiind de până la 100.000 de utilizatori. Ca şi particularităţi de interes tehnic mesajele transmise cu ajutorul aplicaţiei sunt transportate client-server criptat folosind criptare simetrică AES-256, după care sunt salvate la nivelul serverului pentru a putea fi descărcate oricând pe orice alt dispozitiv la care se conectează utilizatorul. Pentru purtarea de conversaţii sigure, aplicaţia pune la dispoziţie opţiunea de conversaţii „secrete”de tip text şi apeluri vocale criptate end-to-end doar între doi utilizatori online, dar nu şi pentru grupuri sau canale cu mai mult de doi utilizatori. Dacă utilizatorul optează pentru acest mod de conversaţie „secretă” atunci mesajele nerecepţionate nu pot fi retrimise destinatarului, iar aceste nu sunt nici salvate pentru back-up. Pe lângă aceste specificaţii aplicaţia atrage controverse prin folosirea unei scheme de criptare proprie derivată din schimbul de chei Diffie-Hellman, care a fost criticată de specialişti. Această schemă de criptare este descrisă pe site-ul celor de la Telegram, purtând numele de protocolul MTProto[7]. Acest protocol este în prezent la versiune 2.0, versiuna MTProto 1.0 fiind considerată depreciată de la sfârşitul anului 2017. Într-o lucrare publicată de Marino Miculan şi Nicola Vitacolonna este făcută o analiză teoretică asupra protocolului MTProto 2.0 şi rezultatul obţinut concluzionează că algoritmul este vulnerabil la anumite tipuri de atacuri MitM [8].

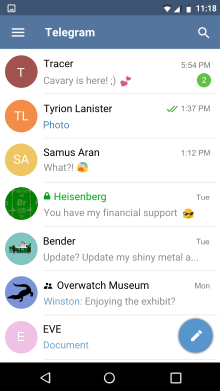


Fig. 4 – Telegram (Versiune de mobil) Homepage [9]

### Google Docs

Google Docs este face parte din suita de aplicaţii şi servicii puse la dispoziţie de către Google. Acest serviciu este accesibil prin intermediul browser-ului de internet ca aplicaţie web, dar este disponibil şi ca aplicaţie mobilă pentru Android, iOS sau desktop doar pe sistemul de operare Chrome OS dezvoltat de Google. Aplicaţia, Google Docs, este destinată pentru realizarea şi editarea de documente online de către mai mulţi utilizatori simultan. Modificările aduse de fiecare utilizator sunt salvate într-un istoric propriu folosit pentru revizuire. Poziţia cursorului specifică fiecărui utilizator este evidenţiată cu ajutorul unei culori, iar un sistem de permisiuni reglementează ceea ce pot face utilizatorii. În plus aplicaţia, dispune de o secţiune specială pentru distribuirea de sarcini către utilizatori, iar modificările aduse fişierelor sunt transmise serverului în mod automat.

Serviciile Google folosesc pentru autentificare şi transport un protocol criptografic numit ALTS, dezvoltat special de Google pentru securizarea servicilor sale, în detrimentul protocolului standard TLS. Ca principale avantaje ale folosirii protocolul ALTS se remarcă utilizarea protocolului de tip buffer (format de date cross-platform gratuit şi open-source destinat serializării datelor) pentru a serializa certificatele şi mesajele de protocol, în timp ce TLS utilizează certificate X.509 codificate cu ASN.1[10].

## Dezvoltarea aplicaţiilor web

## Tehnologii folosite în dezvoltarea aplicaţiilor de tip colaborativ??

# API-uri folosite

## React

## NodeJS

## MySQL

## Socket.Io

## Axios

# Structura proiectului

## Cerinţele sistemului

### Cerinţe funcţionale

### Cerinţe non-funcţionale

## Arhitectura sistemului

### Modulele funcţionale ale sistemului

### Arhitectura aplicaţiei client

#### Diagrame clase

### Arhitectura aplicaţiei server

#### Diagrame Clase

### Persistenţa datelor

#### Diagrama Baza de date

# Implementarea software

## Aplicaţia client

## Aplicaţia web server

### Răspunderea request-urilor

## Implementarea bazei de date

### Diagramă

## Metode de securizare

### Securizarea canalului de comunicaţie

### Criptarea fişierelor stocate

### Protecţie împotriva atacurilor CSRF

### Controlul accesului prin firewall

### Alertare în cazul încercărilor neautorizate

# Utilizarea aplicaţiei

## Actorii sistemului

## Cazurile de utilizare

## Testarea sistemului

## Raport de testare

## Diagrame UML

### Diagrama cazurilor de utilizare

### Diagrama de activităţi

# Concluzii

## Analizarea rezultatelor obţinute

## Dezvoltări ulterioare

# Bibliografie

[1] “What is Collaboration Software?,” Mar. 2021. https://kissflow.com/digital-workplace/collaboration/collaboration-software-guide/ (accessed May 13, 2022).

[2] Shari Kjerland, “Microsoft Teams service description,” 2022. https://docs.microsoft.com/en-us/office365/servicedescriptions/teams-service-description (accessed Jun. 13, 2022).

[3] “Prezentarea experienței Microsoft teams pentru educație simplificată.” https://support.microsoft.com/ro-ro/topic/prezentarea-experien%C8%9Bei-microsoft-teams-pentru-educa%C8%9Bie-simplificat%C4%83-fd5b0668-4156-4ce1-a51a-e6f54827973d (accessed May 13, 2022).

[4] Donna Tam, “Flickr founder plans to kill company e-mails with Slack.” https://www.cnet.com/tech/tech-industry/flickr-founder-plans-to-kill-company-e-mails-with-slack/ (accessed May 13, 2022).

[5] “Slack for Windows.” https://slack.com/downloads/windows (accessed May 13, 2022).

[6] “Discord Support.” https://support.discord.com/hc/en-us/articles/360041721052-Video-Calls (accessed May 13, 2022).

[7] “MTProto Mobile Protocol.” https://core.telegram.org/mtproto (accessed May 13, 2022).

[8] Marino Miculan and Nicola Vitacolonna, “Formal verification of Telegram chat protocol MTProto 2.0.” https://github.com/miculan/telegram-mtproto2-verification (accessed May 13, 2022).

[9] “Telegram Home Page.” https://www.wikidata.org/wiki/Q15616276 (accessed May 13, 2022).

[10] Cesar Ghali, Adam Stubblefield, J. L. Ed Knapp, Benedikt Schmidt, and Julien Boeuf, “Application Layer Transport Security - White Paper”.

# Anexe