

DELTA – Střední škola informatiky a ekonomie, s.r.o.
Ke Kamenci 151, PARDUBICE

DELTA

Střední škola informatiky a ekonomie

P A R D U B I C E

Maturitní projekt

CliSync – Nástroj pro psychology

Příjmení, jméno: MATSENKO Denis

Třída: 4. B

Studijní obor: Informační technologie 18-20-M/01

Školní rok: 2024/2025

1 Zadání maturitního projektu z informatických předmětů

Jméno a příjmení: *Denis Matsenko*
Pro školní rok: *2024/2025*
Třída: *4. B*
Obor: *Informační technologie 18-20-M/01*
Téma práce: *CliSync – Nástroj pro psychology*
Vedoucí práce: *Ing. Tomáš Pešek*

1.1 Způsob zpracování, cíle práce, pokyny k obsahu a rozsahu práce:

- Cílem projektu je vytvořit backend pro aplikaci využívající Next.js API pro práci s klienty správu informací, dat, zapisování proběhlé schůzky jednodušší hledání klientů přes filtry a plánování dalších schůzek. Aplikace poskytne psychologům mnohokrát používající papír a tužku zjednodušenou práci s daty klientů, kontaktních informací a přesune vše spojeno s prací na jedno místo

1.2 Stručný časový harmonogram (s daty a konkretizovanými úkoly):

1.2.1 09.2024 - Nastavení aplikace:

- Nastavení projektu Next.js, databáze .
-

1.2.2 10.2024 – Implementace uživatele, klienta, práce s klienty:

- Vývoj API pro komunikaci s databází.
-

1.2.3 11. 2024 - Implementace security a šifrování:

- sign in, sign up pomocí jwt tokenů, google
- Integrace šifrování citlivých dat

1.2.4 12.2024 – Oprava chyb a leštění:

- Testování a oprava zjištěných chyb.
- Optimalizace výkonu.

Prohlašuji, že jsem maturitní projekt vypracoval samostatně, výhradně s použitím uvedené literatury.

V Pardubicích 1.3.2025

2 Poděkování

Děkuji Ing. Tomáši Peškovi za vedení při tvorbě maturitní práce za jeho poznatky a rady. Také děkuji mým rodičům za její neustálou morální podporu během celého projektu. Nakonec bych chtěl poděkovat Bohu za to že nejsem líný. Děkuji.

3 Anotace

Tato závěrečná práce se zabývá projektem názvem „CliSync“ je v ní popsán postup a použité technologie při tvorbě webové aplikace.

4 Obsah

6	Úvod.....	10
7	VYUŽITÉ TECHNOLOGIE.....	11
1.	VISUAL STUDIO CODE.....	11
2.	MIRO	11
3.	REACT	11
4.	NEXT JS.....	12
1.	Server Side Rendering	12
5.	VERCEL	13
6.	SUPABASE	13
7.	STRIPE	13
8.	GOOGLE CLOUD PLATFORM.....	14
1.	Google authentication	14
2.	Google Calendar API	14
8	NÁVRH DATABÁZE	16
8.1	POPIS DATABÁZOVÉHO SCHÉMATU.....	16
8.2	HLAVNÍ TABULKY A JEJICH ROLE	16
8.2.1	clients	16
8.2.2	sessions.....	16
8.2.3	services.....	17
8.2.4	userServices	17
8.2.5	clientAttachments	17
8.2.6	sessionAttachments	17
8.2.7	tags, tagCategories	17
8.2.8	clientTags	18
8.2.9	passwords	18
8.2.10	googleRefreshTokens	18
8.3	VAZBY MEZI TABULKAMI	18
8.4	NORMALIZACE A OPTIMALIZACE.....	18
9	ARCHITEKTURA.....	20
9.1	HEXAGONAL API. ARCHITECTURE [10].....	20
10	AUTENTIFIKACE	20
10.1	JWT TOKENY.....	20
10.2	BCRYPT	21
10.3	BRUT-FORCE ATTACK (ÚTOK HRUBOU SILOU).....	21

10.4	GOOGLE	21
11	GOOGLE CALENDAR SYNC	21
11.1	AUTORIZACE	22
11.2	SYNCHRONIZACE UDÁLOSTÍ	22
11.3	BEZPEČNOST	22
12	END TO END ŠIFROVÁNÍ.....	22
12.1	JAK FUNGUJE END-TO-END ŠIFROVÁNÍ	22
12.2	DŮLEŽITOST END-TO-END ŠIFROVÁNÍ PRO PSYCHOLOGY.....	23
12.3	REGULACE EU TÝKAJÍCÍ SE END-TO-END ŠIFROVÁNÍ [14]	23
13	TESTOVÁNÍ APLIKACE	23
14	ZÁVĚR.....	23
15	SEZNAM LITERATURY	25

5 Úvod

Aplikace CliSync je moderní nástroj navržený pro zjednodušení administrativní práce psychologů. Mezi psychology nejsou stanovené zásady zapisování informací o klientech. Psychologové často uchovávají data lokálně na počítači, což bývá nezálohované a neorganizované. Stávající pracovní procesy však často zahrnují manuální úkoly, jako je vyhledávání informací o klientech, plánování schůzek v oddělených systémech nebo ruční zapisování poznámek. Tyto činnosti mohou být časově náročné a zbytečně komplikované.

Funkčnost aplikace bude posílena integrací umělé inteligence, která pomůže při zpracování poznámek z konzultací. Umělá inteligence by neměla být používána v aplikacích, kde není její využití opodstatněné. Nicméně v případě práce s textem, například při poznámkách, sumarizaci nebo návrzích na vylepšení textu, představují LLM (Large Language Models) ideální nástroj. Jejich použití v tomto kontextu je smysluplné, protože jsou vytrénované na obrovském množství textů dostupných na internetu a dosahují vysoké úrovně přesnosti [15].

Při tvorbě aplikace byl kladen důraz na zabezpečení. Zabezpečení bude podpořeno vyvinutím vlastního způsobu autentifikace pomocí JWT tokenů a E2EE (End-to-End Encryption), aby k datům neměl přístup nikdo jiný než psycholog – ani vývojáři aplikace. Klíče pro šifrování budou generovány lokálně a nejsou sdíleny mimo zařízení uživatele. Pro dodržení evropských legislativních standardů je veškerá datová infrastruktura umístěna na území EU. [14] Zabezpečení je také hlavní důvod integrace self-hosted AI řešení, aby byly minimalizovány externí závislosti a byla zajištěna maximální ochrana citlivých dat.

Backend aplikace bude postaven s využitím PostgreSQL databáze, hostované na platformě Supabase, což zajišťuje vysoký výkon, škálovatelnost a bezpečnost dat. Supabase přináší snadnou integraci s aplikacemi a poskytuje API pro přístup k datům v reálném čase. Backendová část je navržena tak, aby byla snadno rozšiřitelná a umožňovala integraci s dalšími nástroji.

Backend aplikace bude tvořit:

- **Správa uživatelských dat:** Ukládání a zpracování informací o klientech, schůzkách a poznámkách. Veškeré údaje jsou šifrovány, aby byla zajištěna maximální bezpečnost citlivých dat.
- **Autentizace a autorizace:** Přihlašování uživatelů probíhá prostřednictvím zabezpečených protokolů OAuth 2.0 a JWT tokenů, což umožňuje bezpečný přístup k aplikaci a jejím funkcím.
- **Integrace s externími API:** Backend komunikuje například s Google Kalendářem pro synchronizaci schůzek nebo s AI službami pro přepis mluveného slova a sumarizaci textu.
- **Reakce v reálném čase:** Díky Supabase a WebSocketům mohou být změny dat okamžitě reflektovány v uživatelském rozhraní.
- **Automatizace a notifikace:** Backend generuje upozornění pro uživatele (např. připomínky schůzek) a umožňuje automatické operace, jako je synchronizace kalendáře nebo zálohování dat.

6 Využité technologie

Při vývoji aplikace CliSync bylo využito několik moderních nástrojů a technologií, které umožnily zajistit výkon, škálovatelnost a bezpečnost aplikace. Následující kapitoly představují klíčové technologie a jejich přínos pro projekt.

6.1 Visual Studio Code

Visual Studio Code [1] je open-source editor pro úpravu kódu vyvinutý společností Microsoft, dostupný pro operační systémy Windows, macOS a Linux. Jedná se o výkonný a flexibilní nástroj, který usnadňuje tvorbu, úpravu a správu kódu. Podporuje mnoho programovacích jazyků, čímž se stával univerzálním řešením. Jednou z jeho klíčových vlastností je IntelliSense, což je funkce automatického doplňování kódu, která nabízí chytré návrhy na základě analýzy projektu. Kromě toho obsahuje integrovaný terminál, který umožňuje spouštět příkazy přímo z editoru, a vestavěné nástroje pro ladění, které pomáhají identifikovat a řešit chyby přímo v kódu. Díky podpoře rozšíření lze přidávat nové funkce, například lintování, a podporu pro specifické technologie a frameworky. VS Code je rovněž dobře integrován s Gitem a GitHubem, což usnadňuje spolupráci v týmu, která byla pro náš projekt potřeba. Oblíbený je díky možnosti vytvořit vlastní rozšíření, kvůli kterým z VS Code vytvořila komunita momentálně nejlepší editor. [9]

6.2 Miro

Miro [2] je online platforma pro vizuální spolupráci, která umožňuje týmům pracovat společně v reálném čase nebo asynchronně. Je známá především jako digitální whiteboard, který nabízí širokou škálu nástrojů pro brainstorming, plánování, designování a řízení projektů. Uživatelé mohou vytvářet diagramy, mapy myšlenek, vývojové diagramy, wireframy a mnoho více

Díky intuitivnímu rozhraní a snadnému sdílení umožňuje spolupráci, a to i na dálku. Aplikace je využívána například vývojáři nebo designery. Její klíčovou vlastností je neomezené plátno, na kterém lze vizualizovat složité nápady, strukturovat informace a propojit různé formáty obsahu, což podporuje kreativitu a týmovou produktivitu.

6.3 React

React [3] je open-source JavaScriptová knihovna vyvinutá společností Meta pro tvorbu uživatelských rozhraní. Umožňuje jednoduše a efektivně vytvářet webové aplikace.

Především jsem potřeboval nástroj, který umožní vytvářet uživatelské rozhraní efektivně, flexibilně a škálovatelně. React nabízí komponentový přístup, což umožňuje rozdělit aplikaci na menší, znovupoužitelné části, díky tomu je vývoj nejen rychlejší, ale i jednodušejí a udržitelný přehledně.

Dalším důvodem je Virtuální DOM, který zajišťuje výkon aplikace. React provádí aktualizace uživatelského rozhraní pouze tam, kde došlo ke změnám, což je pro účely aplikace, která

zpracovává obsah dynamicky, jako například kalendář nebo seznam klientů. Deklarativní přístup Reactu pak usnadňuje definici toho, jak má uživatelské rozhraní vypadat v různých stavech, což je ideální pro práci s komplexními daty a různými scénáři interakce uživateli.

Jeden z hlavních důvodů proč je v práci využit react jsou react hooky. Díky hookům, jako je useState nebo useEffect, jsem mohl pracovat se stavem a vedlejšími efekty aplikace jednoduše a bez nutnosti psát třídy, což zrychlilo a zpříjemnilo vývoj.

6.4 Next JS

Next.js [4] je framework postavený nad Reactem, který rozšiřuje možnosti vývoje webových aplikací. Nabízí Server-Side Rendering (SSR) a Static Site Generation (SSG), což vede ke zrychlení načítání stránek a lepší SEO optimalizaci. Například dynamické stránky, jako je seznam klientů nebo kalendář, mohou být vykresleny rychleji a vyhledávače je snadněji indexují. Automatický routing na základě toho jak jsou vytvořeny dokumenty v projektu zjednodušuje správu aplikací, zatímco API Routes umožňuje vytvářet backendové funkce přímo v aplikaci bez potřeby samostatného serveru. Next.js také nabízí Image Optimization, která automaticky optimalizuje velikost a formát obrázků, čímž zlepšuje výkon aplikace a uživatelskou zkušenost, zejména na mobilních zařízeních. Protože je postavený na Reactu, poskytuje všechny jeho výhody, včetně hooků, komponentového přístupu a Virtuálního DOMu, ale přidává pokročilé funkce bez nutnosti složité konfigurace. Navíc má build-in podporu pro TypeScript, což zjednodušuje vývoj a zlepšuje stabilitu kódu.

6.4.1 Server Side Rendering

Server-Side Rendering přináší několik zásadních výhod, zejména pro webové aplikace, které vyžadují vysoký výkon, rychlé načítání obsahu a optimalizaci pro vyhledávače. SSR předrenderuje obsah na serveru, takže uživatel dostane kompletní HTML stránku ještě před načtením JavaScriptu. To znamená, že uživatelé uvidí obsah téměř okamžitě, což zlepšuje uživatelskou zkušenost. Je to zvláště výhodné pro aplikace s obsahem, který se často mění, jako jsou e-shopy, zpravodajské portály nebo dynamické tabulky dat. Dalším důvodem pro použití SSR je lepší SEO. Vyhledávače upřednostňují weby, které servírují plný obsah ve formě HTML, což usnadňuje indexaci a zlepšuje viditelnost webu. SSR také umožňuje generovat personalizované stránky přímo na serveru, například zobrazení uživatelsky specifických dat nebo přizpůsobení obsahu na základě lokalizace či zařízení. Další výhodou je lepší výkon na pomalejších zařízeních, protože většina zátěže je přesunuta na server. SSR lze navíc kombinovat s dalšími strategiemi, jako je Static Site Generation pro statické stránky nebo Client-Side Rendering pro interaktivní prvky. Tato flexibilita umožňuje optimalizovat aplikaci pro různé scénáře, například pro real-time aktualizace obsahu, kdy server načte aktuální data při každém požadavku, a uživatel tak vždy dostane nejnovější verzi. SSR je vhodné, pokud potřebujete lepší SEO, pracujete s dynamickým obsahem, chcete snížit dobu načítání stránky nebo podporovat méně výkonná zařízení.

6.5 Vercel

Vercel [5] je cloudová platforma pro nasazování a škálování moderních webových aplikací. Zaměřuje se na rychlost, jednoduchost a podporu vývojářů

Používání platformy Vercel přináší řadu výhod, které usnadňují vývoj a nasazení webových aplikací, zejména těch postavených na frameworku Next.js. Vercel je navržen tak, aby vývojáři mohli rychle nasazovat své projekty bez složité konfigurace serverů nebo infrastruktury. Jednou z hlavních výhod je možnost nastavení a automatického nasazení z GitHub repozitářů. Při každé změně kódu je aplikace automaticky nasazena na produkční i testovací prostředí. Dalším důvodem je vysoký výkon a optimalizace pro koncové uživatele. Vercel poskytuje globální síť CDN, která zajišťuje rychlé načítání stránek po celém světě. [16] Platforma také nativně podporuje server-side rendering a static site generation, což je perfektní kombinace pro aplikace založené na Next.js. Navíc nabízí funkce jako edge middleware, které umožňují přizpůsobení obsahu přímo na okraji sítě, čímž se zlepšuje uživatelská zkušenost. Velkou výhodou je také jednoduchost a přívětivé rozhraní, které umožňuje monitorovat stav nasazení, výkon aplikace nebo správu domén. Vercel navíc podporuje týmovou spolupráci, což znamená, že více vývojářů může pracovat na jednom projektu efektivněji.

6.6 Supabase

Supabase [6] je open-source alternativa k Firebase, která poskytuje kompletní backend řešení pro moderní aplikace. Nabízí databázi postavenou na PostgreSQL, autentizaci uživatelů, cloudové funkce a real-time synchronizaci dat. Díky své jednoduchosti a výkonnosti je Supabase ideálním nástrojem pro vývoj aplikací bez nutnosti správy vlastního backendu.

Hlavní výhodou Supabase je integrace s PostgreSQL, což umožňuje využívat výhody robustní relační databáze včetně SQL dotazů, indexování a funkcí jako **Row Level Security** pro detailní řízení přístupu k datům. Platforma také nabízí **automatickou generaci API** na základě struktury databáze, což usnadňuje práci s daty bez nutnosti psaní vlastních backendových endpointů.

Dalším klíčovým aspektem je real-time synchronizace, která umožňuje okamžité aktualizace dat v aplikaci, což je ideální pro chatovací aplikace, živé tabulky nebo analytické nástroje. Supabase také poskytuje **vestavěnou autentizaci**, která podporuje přihlášení pomocí emailu, sociálních sítí i externích poskytovatelů OAuth, čímž výrazně zjednodušuje správu uživatelských účtů.

Použití Supabase umožňuje rychle vytvářet a škálovat moderní aplikace s minimální konfigurací. Díky intuitivnímu rozhraní a podpoře TypeScriptu se jedná o skvělou volbu pro vývojáře, kteří hledají flexibilní a výkonné backendové řešení.

6.7 Stripe

Stripe [7] je moderní platební platforma, která umožňuje snadnou a bezpečnou integraci platebních metod do webových a mobilních aplikací. Poskytuje širokou škálu funkcí, včetně zpracování online plateb, předplatného, fakturace a správy financí.

Jednou z hlavních výhod Stripe je **jednoduchá integrace** prostřednictvím přehledného API, které podporuje různé platební metody, jako jsou kreditní a debetní karty, Apple Pay, Google Pay nebo bankovní převody. Stripe také nabízí pokročilé nástroje pro **detekci podvodů** a bezpečnostní mechanismy, jako je **3D Secure** a **tokenizace karet**, což zajišťuje vysokou úroveň ochrany uživatelských údajů.

Dalším významným aspektem je **podpora opakovaných plateb**, což je ideální pro SaaS aplikace a služby založené na předplatném. Stripe umožňuje snadnou správu předplatných, včetně automatického vystavování faktur a sledování platebních cyklů.

Díky **globální dostupnosti** a podpoře více než 135 měn je Stripe vhodný pro mezinárodní platby a obchodování. Platforma navíc poskytuje přehledné analytické nástroje, které umožňují sledovat transakce, výnosy a chování zákazníků v reálném čase.

6.8 Google Cloud Platform

Google cloud platform [8] je služba poskytovaná společností Google, poskytuje sadu nástrojů a služeb, které umožňují integraci různých funkcí. Mezi využívané patří **Google Authentication** pro přihlášení uživatelů a **Google Calendar API** pro práci s kalendářovými událostmi, které byly využity v závěrečné práci.

6.8.1 Google authentication

Google Authentication umožňuje uživatelům přihlašovat se do aplikace pomocí svého Google účtu. Tento způsob přihlášení zvyšuje bezpečnost a zjednodušuje uživatelský zážitek, protože eliminuje potřebu vytvářet nové heslo.

Integrace probíhá prostřednictvím OAuth 2.0, což znamená, že aplikace nikdy nezíská přímý přístup k uživatelskému heslu. Po úspěšném přihlášení obdrží aplikace **OAuth token**, který lze dále využívat k autorizovanému přístupu k dalším Google službám.

Hlavní výhodou je **snadná implementace**, protože Google poskytuje hotové knihovny a SDK pro různé platformy. Autentizace pomocí Google účtu je také **důvěryhodná pro uživatele**, protože využívá ověřenou infrastrukturu Google pro správu identity.

6.8.2 Google Calendar API

Google Calendar API umožňuje aplikacím pracovat s kalendářovými událostmi uživatelů. Pomocí tohoto API lze **vytvářet, aktualizovat, mazat nebo získávat informace o událostech** přímo z Google Kalendáře.

Jednou z klíčových funkcí je **synchronizace v reálném čase**, což umožňuje aplikacím automaticky aktualizovat kalendářová data bez potřeby manuálního obnovení. API také podporuje **nastavení připomenutí, sdílení kalendářů a notifikace o změnách**, což je užitečné pro plánování schůzek, rezervací a dalších událostí.

Google Calendar API je široce využíváno v aplikacích pro **řízení času, projektový management nebo firemní plánování**, kde je potřeba efektivně organizovat schůzky a synchronizovat je mezi více uživateli.

Díky široké funkcionalitě a snadné integraci je Google API skvělou volbou pro aplikace, které chtějí využít sílu ekosystému Google a nabídnout uživatelům komfortní práci s daty a autentizací.

7 Návrh databáze

Navržené databázové schéma poskytuje robustní a škálovatelné řešení pro správu uživatelských dat, klientů a relací. Díky normalizaci a referenční integritě umožňuje efektivní zpracování dotazů a zajišťuje konzistenci dat. Architektura databáze zároveň podporuje budoucí rozšiřitelnost systému.

7.1 Popis databázového schématu

Databázové schéma představuje návrh relační databáze určené pro správu klientů, uživatelů, relací a souvisejících služeb.

7.2 Hlavní tabulky a jejich role

- **users** – Obsahuje informace o uživateli systému. Mezi klíčové atributy patří:
- **id** – Primární klíč uživatele.
- **email** – Emailová adresa uživatele.
- **phoneNumber** – Telefonní číslo uživatele.
- **city, country** – Místo pobytu uživatele.
- **isActive** – Indikátor aktivního účtu.
- **profilePictureUrl** – URL k profilovému obrázku.
- **googleAuth** – Možnost přihlášení přes Google.

7.2.1 clients

Uchovává údaje o klientech, které spravují uživatelé. Mezi klíčové atributy patří:

- **id** – Primární klíč klienta.
- **name, email, phoneNumber** – Identifikační a kontaktní údaje.
- **userId** – Cizí klíč na tabulku users, určující vlastníka klienta.

7.2.2 sessions

Tabulka zaznamenávající jednotlivé relace mezi klientem a uživatelem.

- **id** – Primární klíč relace.
- **clientId** – Cizí klíč na tabulku clients.
- **userId** – Cizí klíč na tabulku users.
- **start, end** – Časové údaje o začátku a konci relace.
- **note** – Poznámka k relaci.

7.2.3 services

Tabulka obsahující informace o nabízených službách.

- **id** – Primární klíč služby.
- **createdAt** – Datum vytvoření služby.

7.2.4 userServices

Spojovací tabulka mezi uživateli a službami, umožňující definovat, jaké služby uživatel nabízí.

- **id** – Primární klíč.
- **userId** – Cizí klíč na tabulku users.
- **serviceId** – Cizí klíč na tabulku services.

7.2.5 clientAttachments

Uchovává soubory nahrané klienty.

- **id** – Primární klíč.
- **clientId** – Cizí klíč na tabulku clients.
- **path** – Cesta k souboru.
- **fullName** – Název souboru.
- **bucket** – Skladovací prostor souboru.

7.2.6 sessionAttachments

Podobná tabulka jako clientAttachments, ale vztahuje se ke konkrétní relaci.

- **id** – Primární klíč.
- **sessionId** – Cizí klíč na tabulku sessions.
- **path, fullName, bucket** – Atributy souboru.

7.2.7 tags, tagCategories

Umožňují kategorizaci klientů či služeb.

tags: obsahuje jednotlivé značky.

tagCategories: definuje kategorie tagů.

7.2.8 clientTags

Spojovací tabulka mezi klienty a jejich značkami.

- **clientId** – Cizí klíč na tabulku clients.
- **tagId** – Cizí klíč na tabulku tags.

7.2.9 passwords

Správa hesel k uživatelským účtům.

- **id** – Primární klíč.
- **userId** – Cizí klíč na tabulku users.
- **saltedPassword** – Zašifrované heslo.

7.2.10 googleRefreshTokens

Obsahuje tokeny pro přístup k externím službám, například Google API.

- **id** – Primární klíč.
- **userId** – Cizí klíč na tabulku users.
- **token** – Hodnota tokenu.

7.3 Vazby mezi tabulkami

Relační struktura databáze zajišťuje logické propojení tabulek a usnadňuje optimalizaci dotazů.

Klíčové vazby jsou:

- Každý uživatel (users) může mít více klientů (clients).
- Každý klient (clients) může mít více relací (sessions).
- Každá relace (sessions) může obsahovat více příloh ve formě sessionsAttachments.
- Služby (services) jsou propojeny s uživateli přes userServices.
- Tagy (tags) jsou spojeny s klienty přes clientTags.

7.4 Normalizace a optimalizace

Databázový návrh byl vytvořen v souladu s principy normalizace:

- 1. normální forma (1NF) – Každý sloupec obsahuje pouze atomické hodnoty.
- 2. normální forma (2NF) – Každá tabulka má primární klíč a neobsahuje redundanci.
- 3. normální forma (3NF) – Neobsahuje tranzitivní závislosti, data jsou rozdělena mezi specifické tabulky.



8 Architektura

8.1 Hexagonal API. architecture [10]

Pro práci s API byla v projektu využita Hexagonal architecture. Tato architektura byla a využita protože kód který je při ní vytvořen je jednoduše znovu využitelný a také pro rozdělení jednotlivých funkcí API do více částí. Architekturu je také možné použít i v případě, že bude nutné změnit některou technologii použitých v projektu.

Hexagonal architecture je architektura která dělí API do 3 základních částí na **Handler**, **Domain** a **Controller**.

- **Handler** přijímá požadavky od klienta (např. http requesty) a předává je. Spravuje autentifikaci, stará se o input validation a convertuje data do typů vhodných pro předání Controlleru.
- **Domain** představuje jádro aplikace a obsahuje veškerou business logiku a pravidla aplikace. V této vrstvě se definují doménové modely, business pravidla a rozhraní (end pointy) pro přístup k databázi nebo externím službám. Domain je zcela nezávislá na konkrétní technologii a neobsahuje žádný kód spojený s API frameworky nebo databázemi.
- **Controller** funguje jako spojovací článek mezi Handlerem a Domain vrstvou. Přijímá požadavky z Handleru, volá potřebnou business logiku v Domain vrstvě a formátuje odpovědi, které následně předává zpět Handleru. Také se stará o zpracování chyb a jejich překlad do odpovědí pro klienta. **Controller** také umožňuje to, že není zapotřebí psát pro každou query do databáze nový endpoint. Každá tabulka v databázi má svůj **Controller**

Celkově pak tento způsob umožňuje vše co bylo v aplikaci potřeba a tvoří škálovatelnou a jednoduše testovatelnou API, udržuje přehledný kód a umožňuje modularitu aplikace, snadno vyměnitelné komponenty aplikace například databázovou technologii.

9 Autentifikace

Správně implementovaná autentifikace je v této aplikaci základní pilíř vzhledem k citlivosti zpracovávaných dat. Autentifikace byla vytvořena bez použití externích řešení nebo řešení třetích stran.

9.1 JWT tokeny

Autentifikace byla implementována pomocí JWT [11] (Json Web Tokenů). JWT je standard pro vytváření šifrovaných dat ve struktuře JSON. Tokeny jsou podepsány pomocí sdíleného tajného nebo veřejného/soukromého klíče.

Server vygeneruje aplikaci token s podrobnostmi přihlášení. Tokeny jsou také podepsány klíčem serveru aby je mohl ověřit. Tokeny jsou kompaktní, bezpečné pro URL

9.2 Bcrypt

Pro hashování přihlašovacích hesel do aplikace byla použita funkce bcrypt [12], je kryptografický algoritmus určený pro bezpečné **hashování hesel**. Používá se k ukládání hesel v databázích tak, aby byla chráněna před úniky a útoky hrubou silou.

Generování hashe probíhá tak, že bcrypt poté co uživatel zadá heslo k němu přidá sůl a použije Blowfish šifru která hash vytvoří.

Bcrypt nabízí možnost iterativně zpomalit hashování a pastavit cost factor (počet opakování výpočtu). To vytváří odolnost proti brute force útoku, protože je útočník nucen opakovaně provádět dlouhé výpočty.

Důvod využití této funkce je aby developer aplikace neměl možnost z databáze vyčíst přihlašovací údaje psychologa a tím nebyl schopen získat přístup k citlivým datům o klientech psychologa.

9.3 Brut-force attack (útok hrubou silou)

Brute-force attack [13] (útok hrubou silou) je metoda, při které útočník systematicky zkouší všechny možné kombinace hesel nebo šifrovacích klíčů, dokud nenajde správnou. Tento přístup je založen na pokusu a omylu a využívá automatizované nástroje, které mohou vyzkoušet velké množství kombinací v krátkém čase.

9.4 Google

Aplikace nabízí možnost přihlášení prostřednictvím Google účtu, což uživatelům poskytuje pohodlný a bezpečný způsob ověření identity. V tomto procesu jsou veškeré požadavky na servery Google odesílány přímo z našeho vlastního API, aniž by bylo využíváno externích řešení třetích stran, jako je například Firebase. Tento přístup nám umožňuje mít plnou kontrolu nad autentizačním procesem a lépe zabezpečit citlivé uživatelské údaje. Po úspěšném přihlášení je uživatel autorizován pomocí JWT tokenů, které zajišťují bezpečné a efektivní ověřování identity při následných požadavcích na API.

10 Google calendar sync

Synchronizace s Google Kalendářem byla implementována pomocí Google Calendar API, které umožňuje propojení aplikace s uživatelskými kalendáři a automatizované plánování událostí.

Proces implementace zahrnoval registraci aplikace v Google Cloud Console, získání přístupových oprávnění od uživatelů a integraci s databází systému.

10.1 Autorizace

Prvním krokem bylo nastavení OAuth 2.0 autentizace, která umožňuje uživatelům bezpečně propojit svůj Google účet s aplikací. Uživatel je při prvním propojení přesměrován na přihlašovací stránku Google, kde musí udělit souhlas s přístupem ke svému kalendáři. Po schválení je vygenerován autorizační kód, který se následně vymění za přístupový a obnovovací token. Tyto tokeny jsou uloženy v databázové tabulce **googleRefreshTokens** a umožňují přístup k API bez nutnosti opakovaného přihlašování.

10.2 Synchronizace událostí

Aplikace umožňuje obousměrnou synchronizaci mezi systémem a Google Kalendářem. Při vytvoření nové relace (**sessions**) v databázi je automaticky odeslán požadavek na Google Calendar API k vytvoření odpovídající události v propojeném kalendáři uživatele. Tato událost obsahuje informace o datu, čase, délce trvání a případné poznámky.

Podobně při úpravě nebo smazání relace v systému dochází k aktualizaci nebo odstranění odpovídající události v Google Kalendáři. Tento proces je zajištěn prostřednictvím jedinečných identifikátorů událostí, které jsou uloženy v databázi a propojují lokální relace s externími událostmi.

10.3 Bezpečnost

Přístupové tokeny jsou pravidelně obnovovány, aby se zabránilo jejich expiraci a uživatelé nemuseli znovu procházet autorizací. Citlivé údaje jsou uloženy šifrovaně a přístupy jsou řízeny pomocí bezpečnostních politik definovaných v Google Cloud Console.

Synchronizace google kalendáře byla pro psychology nutná funkcionalita. Umožňuje psychologům nahlížet do osobního kalendáře přímo z aplikace CliSync.

11 End to end šifrování

11.1 Jak funguje end-to-end šifrování

End-to-end šifrování (E2EE) je bezpečnostní protokol, který zajišťuje, že obsah digitální komunikace je přístupný pouze odesílateli a zamýšlenému příjemci. Při použití E2EE je zpráva šifrována na zařízení odesílatele a dešifrována až na zařízení příjemce, což znemožňuje třetím stranám, včetně poskytovatelů služeb či hackerů, získat přístup k obsahu komunikace.

11.2 Důležitost end-to-end šifrování pro psychology

Pro psychology je ochrana důvěrnosti komunikace s klienty zásadní, protože často pracují s citlivými osobními informacemi. Implementace E2EE v komunikačních nástrojích zajišťuje, že pouze terapeut a klient mají přístup k obsahu jejich konverzací, čímž se minimalizuje riziko neoprávněného přístupu nebo úniku dat. Tato úroveň zabezpečení je klíčová pro udržení důvěry klientů a dodržování profesních standardů týkajících se ochrany soukromí.

11.3 Regulace EU týkající se end-to-end šifrování [14]

Evropská unie klade důraz na ochranu soukromí a bezpečnost komunikace. I když existují návrhy na regulace zaměřené na boj proti zneužívání online platforem, EU neplánuje zakázat end-to-end šifrování. Například návrh Evropské komise zaměřený na boj proti šíření dětské pornografie nepožaduje zákaz E2EE, ale spíše hledá způsoby, jak řešit bezpečnostní rizika, aniž by ohrozil bezpečnost šifrované komunikace.

Implementace E2EE vyžaduje pokročilé technické znalosti a pečlivé plánování, zejména pokud jde o správu šifrovacích klíčů a zajištění kompatibility mezi různými zařízeními a platformami. Přesto je tato implementace nezbytná pro zajištění maximální bezpečnosti a důvěrnosti komunikace. Pro psychology to znamená, že mohou poskytovat své služby s vědomím, že komunikace s klienty je chráněna před neoprávněným přístupem, což je zásadní pro udržení profesionální etiky a dodržování právních předpisů týkajících se ochrany osobních údajů.

12 Testování aplikace

Během vývoje aplikace docházelo ke změnám ve funkcionalitě na základě zpětné vazby od psychologů, se kterými byla uspořádána série sezení. Cílem těchto setkání bylo otestovat aplikaci a zjistit jejich specifické požadavky na funkcionalitu, která je pro jejich každodenní práci nezbytná. Tyto konzultace byly přínosné pro obě strany – umožnily vývojářům nahlédnout na aplikaci z pohledu uživatele bez pokročilých technických znalostí a lépe pochopit potřeby psychologů. Zároveň pomohly identifikovat klíčové funkce, které se z vnějšího pohledu nemusí zdát jako zásadní, ale pro psychology představují nepostradatelný nástroj v jejich profesi.

13 Závěr

Výsledkem projektu je aplikace, která měla za cíl usnadnit práci psychologům, kteří jsou v současnosti velmi vyhledávanou profesní skupinou. V České republice je psychologů nedostatek a rostoucí poptávka vede k dlouhým čekacím lhůtám na terapii, které mohou dosahovat až tří měsíců. Proto bylo v rámci vývoje aplikace absolvováno několik konzultací s psychology, za účelem zjistit, co by jim pomohlo pracovat efektivněji a tím umožnilo za stejný čas pomoci více lidem.

Aplikace obsahuje všechny plánované funkcionality, které byly na základě zpětné vazby identifikovány jako klíčové pro zjednodušení práce psychologů. Hlavním cílem bylo

minimalizovat čas strávený opakovaným vyhledáváním telefonních čísel, starých zápisů nebo jiných informací z předchozích sezení. Což bylo splněno.

Při implementaci aplikace byl vytvořen kalendář, který je propojen s plánovanými schůzkami navázanými na samotné klienty, karta klienta, pro přehledné zobrazení dat. Implementován byl textový editor optimalizovaný pro rychlé a efektivní psaní zápisů ze sezení. Vzhledem k citlivosti zpracovávaných údajů bylo implementováno dvoufaktorové ověření a end-to-end šifrování, pro zajištění maximální bezpečnosti klientských dat.

V budoucnu plánujeme aplikaci rozšířit o nové funkce, jako je podpora mobilních zařízení formou nativní aplikace pro iOS a Android. Zvažujeme také integraci dalších nástrojů, například přímé komunikace s klienty nebo pokročilých analytických funkcí pro sledování vývoje jednotlivých případů. Další rozšíření může zahrnovat rozšíření AI funkcí, jako je predikce potřeb klientů na základě záznamů nebo generování podrobných plánů terapií na míru.

14 Seznam literatury

- [1] Microsoft. *Visual Studio Code*. [online]. [cit. 2025-01-19]. Dostupné z: <https://code.visualstudio.com/>
- [2] Miro. *Miro: Online Whiteboard for Visual Collaboration*. [online]. [cit. 2025-01-19]. Dostupné z: <https://miro.com/>
- [3] Meta Platforms, Inc. *React – A JavaScript library for building user interfaces*. [online]. [cit. 2025-01-19]. Dostupné z: <https://react.dev/>
- [4] Vercel. *Next.js: The React Framework*. [online]. [cit. 2025-01-19]. Dostupné z: <https://nextjs.org/>
- [5] Vercel. Vercel: Develop. Preview. Ship. [online]. [cit. 2025-01-19]. Dostupné z: <https://vercel.com>
- [6] Supabase. Online. 2025. Dostupné z: <https://supabase.com/>. [cit. 2025-03-15].
- [7] Stripe. Online. 2025. Dostupné z: <https://stripe.com/>. [cit. 2025-03-15].
- [8] Google Cloud Platform. Online. 2025. Dostupné z: https://cloud.google.com/gcp?utm_source=google&utm_medium=cpc&utm_campaign=emea-ro-all-ro-bkws-all-all-trial-e-gcp-1707574&utm_content=text-ad-none-any-DEV_c-CRE_548660727720-ADGP_Hybrid+%7C+BKWS+-+EXA+%7C+Txt+-+GCP+-+General+-+v1-KWID_43700060393215959-kwd-26415313501-userloc_2642&utm_term=KW_google%20cloud%20platform-NET_g-PLAC_&&gclid=Cj0KCQjwytS-BhCKARIsAMGJyzpEuaE1Swp3YddOMY06SVcOSV1nrXLwj14vDV_yu7rLryNsTtJcDtwAAsz5EALw_wcB. [cit. 2025-03-15].
- [9] *Stack Overflow*. Online. Stackoverflow.co. 2024. Dostupné z: <https://survey.stackoverflow.co/2024/technology#most-popular-technologies-new-collab-tools>. [cit. 2025-02-27].
- [10] Wikipedia - *Hexagonal architectire*. Online. 2024. Dostupné z: [https://en.wikipedia.org/wiki/Hexagonal_architecture_\(software\)](https://en.wikipedia.org/wiki/Hexagonal_architecture_(software)). [cit. 2025-03-15].
- [11] *Jwt.io*. Online. 2025. Dostupné z: <https://jwt.io/>. [cit. 2025-03-15].
- [12] Wikipedia - *Bcrypt*. Online. 2025. Dostupné z: <https://en.wikipedia.org/wiki/Bcrypt>. [cit. 2025-03-15].
- [13] Wikipedia - *Brute force attack*. Online. 2025. Dostupné z: https://en.wikipedia.org/wiki/Brute-force_attack. [cit. 2025-03-15].

[14] *Europa EU*. Online. Europa.eu. 2024. Dostupné z:
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm. [cit. 2025-02-27].

[15] _Originality.ai What LLM is the most accurate_. Online. Originality.ai. 2024. Dostupné z:
<https://originality.ai/blog/what-llm-is-the-most-accurate> [cit. 2025-02-18].

[16] Vercel Infrastructure. Online. Stackoverflow.co. 2023. Dostupné z:
<https://vercel.com/blog/behind-the-scenes-of-vercel-infrastructure>. [cit. 2025-02-27].