



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ

DEPARTMENT OF COMPUTER SYSTEMS

DOCHÁZKOVÝ SYSTÉM ZAMĚSTNANCŮ

EMPLOYEE ATTENDANCE SYSTEM

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

JAN BARTOŠEK

VEDOUcí PRÁCE

SUPERVISOR

Ing. JITKA KOCNOVÁ

BRNO 2020

Zadání bakalářské práce



Student: **Bartošek Jan**
Program: Informační technologie
Název: **Docházkový systém zaměstnanců**
Employee Attendance System
Kategorie: Informační systémy

Zadání:

1. Prozkoumejte současnou nabídku trhu v oblasti docházkových systémů a seznamte se s nejčastěji používanými metodami pro identifikaci osob.
2. Navrhněte realizaci docházkového systému umožňujícího sledování docházky, plánování dovolené a export dat v otevřeném formátu.
3. Navržený systém implementujte.
4. Systém otestujte, zhodnoťte dosažené výsledky a navrhněte vhodná další rozšíření.

Literatura:

- Dle pokynů vedoucího.

Pro udělení zápočtu za první semestr je požadováno:

- Splnění bodů 1 a 2 zadání.

Podrobné závazné pokyny pro vypracování práce viz <https://www.fit.vut.cz/study/theses/>

Vedoucí práce: **Kocnová Jitka, Ing.**
Vedoucí ústavu: Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání: 1. listopadu 2019
Datum odevzdání: 28. května 2020
Datum schválení: 25. října 2019

Abstrakt

Tato bakalářská práce se zabývá návrhem a implementací docházkového systému pro záznam příchodů a odchodů zaměstnanců ve firmě. V první části definuje, co docházkový systém znamená, a nastíní jak statistické údaje, tak již existující řešení. V další části se zaměřuje na návrh docházkového systému schopného stopování zaměstnanců, správy dovolené a exportování záznamů. Následuje seznam použitých technologií a popis vlastního řešení. Nakonec je uveden proces a výsledky testování.

Abstract

This bachelor's thesis concerns to design and implementation of a time and attendance system to track the employees in the company. In the first part defines what does a time and attendance system mean and presents both statistics data and existing systems. In the next part aims on designing such a software able to track employees, manage vacation and export records. Continues with a list of used technologies and implementation of the system itself. At the end the process and results of testing the system are described.

Klíčová slova

docházkový systém, Docker, NodeJs, Javascript, MySQL, webová aplikace, JavaScript

Keywords

time and attendance system, Docker, NodeJs, MySQL, web application, JavaScript

Citace

BARTOŠEK, Jan. *Docházkový systém zaměstnanců*. Brno, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Jitka Kocnová

Docházkový systém zaměstnanců

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Jitky Kocnové. Uvedl jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpal.

.....

Jan Bartošek
27. května 2020

Poděkování

Chtěl bych poděkovat vedoucí mé práce, Ing. Jitce Kocnové za všechny nápady, rady a postřehy, kterými mě po celou dobu vývoje směřovala správným směrem. Právě díky jejímu dohledu a ochotě se mi podařilo práci vypracovat do takové podoby, v jaké se dnes nachází.

Obsah

1	Úvod	3
2	Docházkové systémy	4
2.1	Identifikace osoby	5
2.1.1	Ověření heslem	6
2.1.2	Ověření čipem	8
2.1.3	Ověření otiskem prstu	10
2.2	Zákonné povinnosti systému	13
2.3	Srovnání používaných systémů	14
3	Návrh systému	17
3.1	Základní komponenty systému	17
3.2	Uživatelské role	20
3.2.1	Diagram případů užití	21
3.3	Grafické rozhraní	23
4	Implementace	24
4.1	Použité technologie	24
4.2	Kontejner	26
4.3	Databáze	26
4.3.1	Model databáze	28
4.3.2	Záloha a obnovení dat	30
4.4	Serverová aplikace	30
4.5	Make	31
5	Testování	32
5.1	Nasazení na fakultním serveru	32
5.2	Nasazení v reálném prostředí	33
5.3	Výsledky testování	34
6	Závěr	35
6.1	Budoucí práce	35
	Literatura	37
A	Obsah CD	39

Seznam obrázků

2.1	Deset nejčastěji používaných hesel. [1]	7
2.2	Ukázka funkčnosti pasivního transpodéru. [2], [3]	9
2.3	Ukázka funkčnosti aktivního transpodéru. [4], [5]	9
2.4	Otisk prstu. [6]	11
2.5	Schéma optického senzoru.	11
2.6	Schéma kapacitního senzoru.	12
2.7	Schéma tepelného senzoru.	12
2.8	Schéma ultrazvukového senzoru.	13
2.9	Rozdělení velikosti společnosti dotázaných zaměstnanců.	14
2.10	Způsoby přihlašování zaměstnanců.	15
2.11	Existence docházkového systému dotázaných.	15
2.12	Spokojenost dotázaných s jejich docházkovými systémy.	15
3.1	Priorita záznamů.	18
3.2	Diagram případů použití.	21
3.3	Návrh grafického rozhraní.	23
4.1	Model logického návrhu databáze.	28

Kapitola 1

Úvod

Tato práce vznikla za účelem vytvoření docházkového systému zaměstnanců určeného pro menší i středně velké firmy. Docházkové systémy řeší především problémy se zápisem časových údajů o docházce a uchováním dat o zaměstnancích na pracovišti. Jejich použití může být však mnohem rozsáhlejší. Můžeme se setkat s docházkovými systémy, které poskytují zabezpečení objektu, rozhraní pro zaměstnance se správou osobních údajů a další. Tak či onak, docházkový systém značně usnadňuje práci zaměstnavatelům a především oddělení lidských zdrojů. Shromážděná data totiž přesně vypovídají o prezenci každého ze zaměstnanců, jejich přesčasových hodinách i absencích. Přesné časové údaje o odpracovaném čase lze využít k výpočtu mzdy, stravenek i dovolené.

Jak se v následujících kapitolách dočteme, spousta společností používá zastaralé způsoby kontroly docházky, jako jsou například sdílené soubory pro zápis příchodů a odchodů, kontrola u povolané osoby nebo dokonce i zapisování do papírových archů. Avšak tyto způsoby s sebou obvykle nesou problémy a úskalí jako jsou například složitá administrativa, špatná detekce a opravení chyby nebo zbytečné vytížení pracovních sil.

V kapitole 2 se dočteme, co to docházkové systémy jsou, jak se klasifikují a jaké způsoby přihlášení uživatele existují, jejich výhody i nevýhody, a především jakou úroveň zabezpečení poskytují. Dále se zaměříme na povinnosti docházkových systémů vyplývajících ze zákoníku práce a v závěru této kapitoly se podíváme na porovnání existujících docházkových systémů. Následuje kapitola 3, kde je uveden seznam použitých technologií a jejich vzájemné propojení. Stejně tak se v této kapitole podíváme na grafický návrh a rozložení uživatelského prostředí. V další kapitole 4 se nachází detailní popis postupu řešení a ukázka chování tohoto docházkového systému. Krátce bude zmíněno testování v kapitole 5 a na závěr se v kapitole 6 podíváme na shrnutí celé práce a rozšíření tohoto docházkového systému.

Kapitola 2

Docházkové systémy

Docházkový systém (angl. Time and Attendance System) je systém, který umožňuje zaznamenávat, uchovávat a pracovat s daty o pohybu zaměstnanců na pracovišti. Mezi tyto pohyby patří především záznamy o příchodu a odchodu do práce, začátek a konec obědové pauzy, čas strávený na pracovní cestě nebo jiné důvody nepřítomnosti zaměstnance. Správně navržený docházkový systém pak umožňuje zaměstnavateli například sledovat aktuální přítomnost jednotlivých zaměstnanců nebo jednoduše odhalit pozdní příchody a neschválené absence. Díky přesnému časovému záznamu je možno snáze spočítat množství přesčasu nebo chybějící hodiny při měsíční uzavírce. Export dat z docházkového systému může být podnětem pro vyplácení mzdy, výdej stravenek nebo výpočet dovolené.

Hlavními výhodami nasazení docházkového systému ve firmě jsou:

1. Zvýšení přesnosti sledování času a docházky zaměstnanců.

Zatímco docházkový systém vždy zaznamená přesný časový údaj, ruční zadávání oproti tomu může snadno zanést chyby, například o odpracovaných hodinách jednotlivých zaměstnanců. Tyto chyby by pak ve výsledku mohly mít velký vliv na skutečně odpracovaný čas a znamenat ztrátu peněz pro firmu i pro zaměstnance.

2. Zefektivnění práce oddělení lidských zdrojů.

Ruční zapisování odpracovaných hodin a s tím spojená administrativa je v případě menšího počtu zaměstnanců zdržující, v případě velkého počtu zaměstnanců dokonce téměř nereálná. Docházkový systém tuto problematiku odstraňuje a šetří personální čas, který může věnovat jiným aspektům ve firmě.

3. Zaměstnanci mají přístup ke svým záznamům o docházce.

Všichni zaměstnanci jistě ocení možnost mít přístup ke svým vlastním údajům, vidět svůj týdenní přehled a měsíční záznamy. V přehledu jim však může být k dispozici i plánovaná dovolená, státní svátky nebo firemní volna.

4. Všechny formality jsou v bezpečí.

Docházkové systémy dokáží exportovat uložená data a vytvářet jejich zálohy jako prevenci proti případné ztrátě. Zákon udává povinnost archivovat záznamy docházky u všech zaměstnanců po dobu 3 let, a právě správný docházkový systém si s touto administrativou musí poradit.

2.1 Identifikace osoby

Hlavní činností docházkového systému je bezesporu přihlášení zaměstnance do systému. Tato akce zaznamená časový údaj o jeho příchodu nebo odchodu. K přihlášení může sloužit přístupový terminál, tím je myšleno zařízení přímo určené k přihlášení zaměstnance, nebo počítačový program, do kterého se zaměstnanec při začátku své pracovní směny přihlásí. Společně s přihlášením je nutno provést ověření totožnosti dané osoby, a tím zjistit jestli člověk, který se pokouší přihlásit je opravdu tím, za koho se vydává. S ověřením totožnosti se pojí následující výrazy: [17]

- **Autentizace** (angl. authentication) je proces, při kterém dochází k verifikaci identity osoby. Osoba v tomto případě předkládá systému prvky, pomocí kterých je systém schopen ověřit identitu (heslo, PIN, čipovou kartu, biometrický vzorek, atd).
- **Identifikace** (angl. identification), stejně jako autentizace, ověřuje identitu osoby. Rozdíl je však v tom, že při identifikaci nepředkládá uživatel žádné prvky a rozpoznání osoby provádí systém prohledáváním databáze uživatelů a hledáním shody.
- **Autorizace** (angl. authorization) je výstupem obou uvedených způsobů. Při úspěšném ověření identity je uživateli autorizován přístup, a on tak může pokračovat dále do systému, vstoupit do budovy nebo jinak nakládat s právy, které mu systém poskytuje. Jakmile je uživateli udělena autorizace, tak se již dále totožnost neověřuje.

Používají se čtyři různé způsoby, kterými se ověřuje totožnost osoby. Každý z těchto způsobů má své klady i zápory a liší se od sebe například úrovní zabezpečení, přenositelností a dalšími faktory. Ověření je nepřenositelné v případě, že uživatel nemůže předat přístup někomu jinému (heslo lze předat, otisk prstu nikoliv). Prokázat danou osobu lze podle:

- **Znalostí uživatele**

Uživatel zná specifickou frázi, heslo nebo pin, pomocí kterých může prokázat svoji identitu. Frázi (angl. passphrase) se rozumí obvykle posloupnost slov, je tedy delší než klasické heslo a poskytuje vyšší zabezpečení. Heslo (angl. password) je většinou jednoslovný řetězec neobsahující znak mezery. PIN je označení pro osobní identifikační číslo (angl. personal identification number) a jedná se tedy pouze o číselný kód. V porovnání s frází nebo heslem poskytuje nejnižší úroveň zabezpečení. Bezpečnost autentizace však závisí na mnoha faktorech. Uživatel si musí zvolit dostatečně silné heslo, které nebude jednoduché uhádnout cizí osobou. Stejně tak je uživatel povinen dané heslo chránit, aby jej nikdo jiný nezjistil. Heslo je však možno odcizit i ze systému, ke kterému se uživatel přihlašuje. Tento systém totiž musí mít uloženou kopii hesla, aby mohl provést ověření a porovnat hodnotu s heslem, kterým se uživatel prokazuje. Proto systémy, které ověřují identitu za pomoci hesla, mají uložený pouze zakódovaný řetězec, který dané heslo reprezentuje. Tomuto řetězci se říká hash a vznikne zašifrováním původního hesla použitím jednosměrné šifry. Jednosměrná je proto, jelikož ze vzniklého hashe již nelze získat originální řetězec. Pokud by se tedy potenciální útočník dokázal dostat k datům uloženým v systému, tak se dočte pouze zmíněného hashe a neměl by být schopen rozluštit původní heslo.

- **Vlastností uživatele**

Vlastností uživatele jsou myšleny specifické rysy, kterými uživatel disponuje. Ověřit totožnost osoby na základě těchto rysů lze právě z důvodu, že pro většinu lidí jsou

tyto rysy ojedinělými nebo alespoň velice vzácnými. Vědní obor, který se zkoumáním těchto rysů zabývá, se jmenuje biometrie [21] a zaměřuje se především studiem a pozorováním živých organismů, především člověka, a na měření jeho biologických vlastností a chování. Díky poznatkům z biometrie dokážeme používat metody vedoucí k rozpoznávání člověka na základě jeho unikátních proporcí nebo vlastností. Těchto metod je velké množství, patří k nim například geometrie ruky nebo tváře, duhovka oka, sítnice oka, způsob pohybu očí nebo topografie rohovky, struktura žil na zápěstí, tvar článku prstu a pěsti, vrásnění článků prstů, dynamika podpisu, dynamika chůze, otisk prstu, akustická charakteristika hlasu, pach, DNA, tvar ušního boltce, tvar a pohyb rtů, rýhování nehtů, spektroskopie kůže, dynamika uchopení a stisku střelné zbraně, podpis nebo vlastnosti zubů. Ověřování na základě biometrických informací obvykle poskytuje vysokou úroveň zabezpečení. Všechny tyto metody jsou navíc nepřenosné.

- **Schopností uživatele**

Uživatel je schopen například odpovědět na sadu vygenerovaných otázek, označit objekt na obrázku, pojmenovat barvu nebo jiným způsobem prokázat své schopnosti či dovednosti. Tato metoda se často používá jako dodatečná ochrana v kombinaci s heslem nebo jiným ověřením, protože sama o sobě neposkytuje vysokou úroveň zabezpečení. V případě, že je použita sama, se s velkou pravděpodobností jedná o test CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) [14], který pouze rozlišuje, zda-li uživatel, jenž se snaží vstoupit do systému, je živou osobou a nikoliv pouze počítačovým programem.

- **Vlastnictvím uživatele**

Uživatel se ověřuje za pomoci specifického, jím vlastněného předmětu. Takový předmět se označuje slovem token a při ověřování osoby tímto tokenem musí systém disponovat čtecím zařízením, které je s tokenem kompatibilní. Rozlišovat lze tvar předmětu nebo data, která jsou v něm uložena. Příkladem ověření za pomoci tvaru může být bankomat a platební karta, která musí velikostí i tvarem odpovídat otvoru v bankomatu. Pokud se předmět do čtecího zařízení nevkládá, tak jej stačí pouze přiblížit. V takových případech token vysílá data, která čtecí zařízení snímá a kontroluje.

Předměty bývají malé, skladné a lehké přenositelné. Zajišťují vysokou míru zabezpečení, především proto, protože se často používají v kombinaci s heslem nebo pinem. Nevýhodou však může být možnost předmět ztratit nebo jej odcizit a následně zneužít.

Nejčastějším typem tokenu je tzv. Smart Card. Tento druh tokenu obsahuje buď magnetický proužek, čip nebo obojí a může být jak kontaktní, tak i bezkontaktní. Používá se tvar karty (velikost 85,60 x 53,98 mm - platební karta) nebo čip v plastovém ochranném krytu kompaktních rozměrů (například klíčenka ve tvaru slzy).

V této práci se budeme zabývat pouze takovými metodami ověření osob, které jsou běžně používané v praxi u docházkových systémů. Jsou jimi ověření pomocí hesla, čipu nebo otisku prstu.

2.1.1 Ověření heslem

Používání hesla je jedním z nejjednodušších a přesto nejrozšířenějších způsobů ověřování identity. Základem této metody je znalost klíče, který je pro ostatní uživatele tajný. Uživatel

je vyzván k vložení tohoto klíče (hesla, PINu) do systému, a pokud je klíč ověřen jako správný pro daného uživatele, tak je mu autorizován vstup do systému.

Hesla jsou dnes využívána tak hojně, že běžný uživatel je nucen pamatovat si velké množství různých hesel. Zde však nastává boj mezi jednoduchostí pro uživatele, a tedy použitím jednoduchého hesla, nebo maximálního zabezpečení, a tedy použitím komplexního, leč špatně zapamatovatelného hesla.

Správné zásady vytvoření hesla

Úroveň zabezpečení při použití hesla je přímo úměrné složitostí hesla. Existuje velká řada metod na prolomení útoku, kdy se útočník snaží uhodnout heslo jiného uživatele, jako je například použití hrubé síly (angl. brutal force attack), použití slovníkového útoku (angl. dictionary attack) nebo použití nějakého triku (angl. phishing). Hrubá síla spočívá v pouhém tipování hesla bez použití sofistikovanější logiky. Slovníkový útok pak vychází z tipování na základě nejběžněji používaných hesel. Posledním způsobem může být situace, kdy útočník pošle uživateli falešný email se zprávou, že s jeho účtem je něco v nepořádku a je potřeba aktualizovat heslo. Zpráva poté obsahuje odkaz na web vypadající například přesně jako web jeho internetového bankovníctví. Jedná se však o podvrh a pokud uživatel heslo ve formuláři vyplní, tak jej pošle přímo útočníkovi.

Obranou před útoky je obezřetnost a silné heslo. Charlotte Empey, marketingová ředitelka společnosti Avast a propagátorka zabezpečení a ochrany soukromí vydala na webu blog.avast.com správné zásady a časté omyly při používání hesel. Na základě tohoto článku by každé heslo mělo dodržovat následující pravidla: [16]

- **Délka** by neměla být kratší než 15 znaků. Ještě delší je však lepší.
- **Kombinace znaků** velkých a malých písmen, číslic a speciálních symbolů.
- **Běžné nahrazení písmen čísly** dnes není pro útočníky takový problém. Hesla jako "K0L0B3ZK4", které vznikne transformací slova "koloběžka" není pro útočníka velkou překážkou.
- **Heslo podle rozložení klávesnice** jako například "qwerty" nebo různé posloupnosti číslic patří k prvním možnostem, které útočník vyzkouší.

Zde je seznam nejběžnějších deseti hesel, které by uživatelé používat neměli.

1	123456
2	123456789
3	qwerty
4	111111
5	password
6	12345678
7	abc123
8	1234567
9	password1
10	123123

Obrázek 2.1: Deset nejčastěji používaných hesel. [1]

Zabezpečení hesla

Nejen uživatel musí držet heslo v tajnosti. Stejně tak systém, ke kterému se uživatel přihlašuje, musí mít uloženou kopii správného hesla, aby mohl porovnat shodu a autorizovat přístup. Heslo se tedy musí chránit před odcizením a zneužitím i na straně systému. Z tohoto důvodu se v systému neukládá heslo v běžné textové podobě, protože kdokoli s přístupem k těmto datům by věděl, jaké heslo uživatelé používají. Místo toho se v systému ukládá šifra původního hesla.

Tato šifra (hash) je speciální řetězec konstantní délky, který vznikne z původního hesla použitím šifrovací metody (komplexní matematické funkce). Pokud tedy máme například heslo "hello", tak jeho šifra může odpovídat hodnotě "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824". Systém tedy při každé autentizaci zašifruje heslo, které uživatel zadá a použije k tomu stejnou šifrovací metodu, kterou použil při vytváření hesla. Poté se porovnávají jednotlivé šifry a v případě shody je uživatel autorizován. Šifrovacích metod existuje mnoho a dělí se dle typu šifrování na jednosměrnou nebo obousměrnou. Pro ukládání hesel se používají výhradně jednosměrné šifry, tedy takové, které z vytvořené šifry nedokáží získat původní heslo. Pokud tedy má člověk přístup k systému, tak by při pohledu na uloženou šifru neměl být schopen zjistit původní heslo.

V tomto případě pomohou útočníkovi tzv. "vyhledávací tabulky" (angl. lookup tables). Tyto tabulky obsahují obrovský seznam šifer pro nejběžnější hesla při použití běžných šifrovacích metod. Útočník si pak může nalézt požadovanou šifru a hned uvidí heslo, které jí odpovídá. Jako obrana před vyhledáním šifry v tabulce se k heslu přidává speciální hodnota, která udělá každé heslo speciálním a minimalizuje tak šanci, že dané heslo se bude nacházet v tabulce. Tomuto řetězci, který konstantně přidáme k uživatelskému heslu se říká sůl. Osolením hesla přidáme sůl k heslu a vytvoříme mnohem bezpečnější heslo. Tato sůl je v ideálním případě hodnota generovaná pro každého uživatele individuálně. Přidáním takto vytvořené soli docílíme jedinečnosti hesel i pro uživatele, kteří si původně zvolili totožná hesla. Pokud k našemu vzorovému heslu "hello" přidáme sůl "QxLUF1bgIAdeQX", tak nám vznikne "helloQxLUF1bgIAdeQX"s šifrou

"9e209040c863f84a31e719795b2577523954739fe5ed3b58a75cff2127075ed1".

Pokud takto zabezpečíme heslo, tak posledním způsobem útočníka je použití hrubé síly. Moderní nejvýkonnější hardware však dokáže generovat biliony šifer v krátkém čase a heslo lze tímto způsobem stále uhodnout rychle. Můžeme však tento způsob výrazně zpomalit, pokud zpomalíme šifrovací metodu, která se spustí při každé autentikaci. Tím omezíme rychlost, se kterou může útočník zkoušet heslo prolomit. Této praxe se říká anglicky key stretching a ideální doba, na kterou bychom měli šifrovací metodu protáhnout, je asi půl vteřiny. Je potřeba totiž nalézt balanc mezi omezením útočníka a zároveň plynulým přihlášením běžného uživatele systému. [22]

2.1.2 Ověření čipem

Použití čipu s sebou přináší výhody v jednoduchém a rychlém ověření dané osoby. Avšak mezi nevýhody patří například povinnost nosit čip s sebou a s tím nutně ošetření případů, kdy si zaměstnanec svůj čip zapomene.

V praxi se realizace takového čipu provádí dvěma metodami, a to především pomocí RFID (Radio Frequency Identification) nebo NFC (Near Field Communication).

Radio Frequency Identification

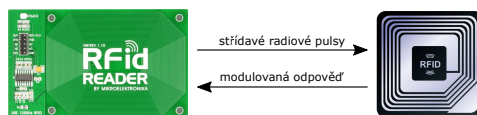
Jedná se o bezdrátový a bezkontaktní systém identifikace za pomoci rádiové frekvence, který díky svým vlastnostem pomalu nahrazuje dříve používané systémy a hojně se využívá například k identifikaci osob nebo sledování zboží. [24, 20]

Hlavními výhodami je například absence vizuálního kontaktu, rychlá obsluha velkého počtu zařízení nebo sledování objektu v reálném čase. RFID čipy se objevují nejčastěji v systémech identifikujících osoby, umožňujících přístupy do budov a areálů, pro sledování zboží a dalších. Pomalu nahrazují čárové kódy a magnetické proužky, oproti kterým umožňují čtení dat i bez přímého vizuálního kontaktu a rychlejší obsluhu většího počtu zařízení najednou. Na zmíněné čárové kódy však ztrácí v hledisku výrobní ceny, kdy vytvoření čipu je nákladnější než-li tisk kódu. Celková velikost je závislá na frekvenci a s ní souvisejícím provedení komunikační antény. [12, 13]

Komunikace vzniká mezi RFID transpondérem (tagem) a čtecím zařízením. Tato komunikace se dělí v závislosti na napájení transpondéru. Ten může být buď pasivní nebo aktivní.

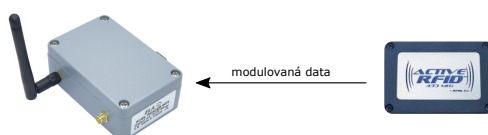
1. **Pasivní transpondér** nemá vlastní zdroj napájení a energii mu musí dodat čtecí zařízení. Toto čtecí zařízení používá elektromagnetické pole a periodicky vysílá do svého okolí elektromagnetickou vlnu na určité frekvenci. Pokud se v dostatečném dosahu nachází pasivní transpondér naslouchající na stejné frekvenci, tak přijme signál a na anténě se indukuje napětí, které slouží jako napájení. Jakmile se nashromáždí dostatečné množství energie, tak komunikační anténa začne odpovídat zpět čtecímu zařízení vysláním dat uložených v paměti transpondéru. [12]

Pasivní provedení je mnohem častější z důvodů nižších pořizovacích nákladů, které vyplývají z absence zdroje elektrické energie v transpodéru. Tento typ dosahuje velice dlouhé životnosti, ale jeho dosah je značně omezený (maximum do jednoho metru).



Obrázek 2.2: Ukázka funkčnosti pasivního transpodéru. [2], [3]

2. **Aktivní transpondér** na rozdíl od pasivního transpodéru obsahuje vlastní napájecí zdroj a čtecí zařízení nemusí vysílat elektromagnetickou vlnu k jeho napájení. Baterie pohání mikročip a posiluje dosah vysílaného signálu. Ten tak dosahuje vzdálenosti až stovky metrů v závislosti na frekvenci a výkonu antény. Aktivní transpodér kontroluje, jestli se v dosahu signálu nachází nějaké čtecí zařízení a při úspěšném nalezení začne vysílat data. Nevýhodou je vysoká pořizovací cena a nižší životnost ovlivněna kapacitou baterie. [12]



Obrázek 2.3: Ukázka funkčnosti aktivního transpodéru. [4], [5]

RFID tagy se dále dělí podle použité paměti na:

1. **Paměť pouze pro čtení (Read only memory)**, tento typ paměti je naprogramován při výrobě a dodatečná úprava již není možná a data je možno pouze číst.
2. **Paměť pouze pro čtení s naprogramováním výchozího stavu (Write once read many memory)** se vyrobí s prázdnou pamětí a první zápis je možno udělat až později. Po naprogramování lze data pouze číst. Princip je podobný jako u disků CD-ROM.
3. **Paměť pro čtení i zápis (Read write memory)** umožňuje opětovné přeprogramování paměti. Udává se celkový počet až tisíce cyklů přepisu. Princip je podobný jako u disků CD-RW.

Liší se i podle použití, kdy se můžeme setkat s RFID tagy připevněnými na lepící papír (použití k jednoduchému označení zboží), chytrými kartami (tzv. SMART card), které jsou známé hlavně jako bezkontaktní platební karta, klíčenky a další. Technologie RFID má dnes využití ve spoustě oblastí. Může sloužit pro kontrolu zboží, oprávnění vstupu do areálu, identifikace osob a dalších. Podle použití se liší i čtecí zařízení, které zvládá mimo dodávání energie pasivním transpondérům i obsluhu velkého počtu signálů najednou, podporu šifrování a zajištění integrity dat. [20]

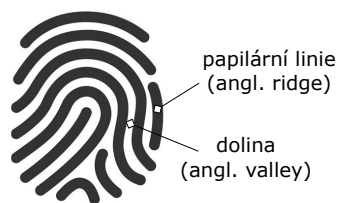
Near Field Communication

Je technologie postavena na základech RFID. Na rozdíl od RFID však slouží k přenosu libovolných informací, kde RFID vysílá pouze informace o sobě, identifikační číslo, apod. NFC komunikuje pouze na velmi krátké vzdálenosti v řádech centimetrů a dosahuje přenosové rychlosti od 106 kbit/s do 424 kbit/s. Za technologiemi jako je WiFi nebo Bluetooth tedy výrazně zaostává, nicméně není primárně použita pro přenosy velkého množství dat. [23, 20]

Nejvíce se technologie NFC používá v telefonech pro uskutečnění bezkontaktní platby. Tato platba je provedena za pomoci aplikace pro správu debetních/platebních karet (Google Pay aj.). Technologie NFC se rychle rozšířila a dnes je tímto způsobem možné platit téměř v každém supermarketu a běžných podnicích, které akceptují bezkontaktní platbu debetní nebo kreditní kartou. Využití však sahá mnohem dál. NFC najdeme například v občanském průkazu, řidičském průkazu, elektronických klíčích, ke konfiguraci Wifi či Bluetooth přenosu a mnoho dalšího. [20]

2.1.3 Ověření otiskem prstu

Otisk prstu je speciální uspořádání papilárních linií na konci každého prstu všech lidí. Jedná se o vyvýšené reliéfy o výšce 0,1–0,4 mm a šířce 0,2–0,7 mm, které se tvarují do stálých obrazců, tzv. dermatoglyfů, a připomínají tvar spirály nebo smyčky. Vědní obor zabývající se těmito liniemi se nazývá daktyloskopie a je postaven na třech zákonech. [18]



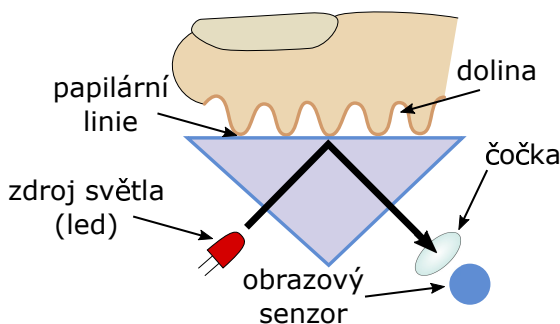
Obrázek 2.4: Otisk prstu. [6]

1. **Zákon o relativní neměnnosti obrazců papilárních linií** říká, že tvar i pozice papilárních linií se v průběhu života nemění a zůstává stále stejný. Vzor papilárních linií jedince je stejný od jeho narození až do dospělosti. Jejich velikost a mezery mezi nimi se z důvodu růstu zvětšují, ale obrazec, který vytváří, zůstává stále stejný. Díky tomuto lze identifikovat za pomoci otisku prstu osobu i po uplynutí velmi dlouhé doby.
2. **Zákon o relativní neodstranitelnosti papilárních linií** uvádí skutečnost, že papilární linie nelze odstranit, změnit nebo jinak deformovat. Při poškození kůže se mohou dočasně poškodit, ale vždy se zahojí do původního stavu.
3. **Zákon o relativní individuálnosti obrazců papilárních linií** potvrzuje, že na světě neexistují dva jedinci se stejnými otisky prstu. Při výpočtu všech možných tvarů papilárních linií mnozí vědci dospěli k tak obrovskému počtu možných kombinací (až 64 miliard různých variant), že šance na shodu je prakticky nulová. [25]

Použití otisku prstu k ověření totožnosti uživatele je nejpoužívanější metoda ze skupiny biometrických způsobů ověřování. Jeho použití se hojně využívá v kriminalistice, administrativní a politické práci, finanční transakci a je nejvíce zastoupeným přístupem k chráněným objektům.

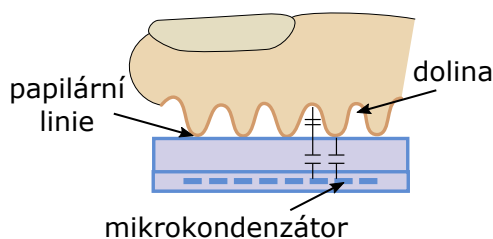
K ověření osoby podle otisku prstu se musí pořídit snímek otisku prstu uživatele, který se pokouší o autorizaci. Používají se čtyři typy senzorů, které otisk prstu snímají. [15, 19]

1. **Optické senzory** (angl. optical sensors) jsou nejstaršími používanými senzory pro snímání otisku prstu. Neposkytují však nejvyšší úroveň zabezpečení. Snímek prstu je pořízen za pomoci lomu světla z diody po odrazu od plochy, ke které je přiložen testovaný otisk. V místech, kde se nachází papilární linie, se světlo neodráží, a naopak v místě, kde se nachází dolina se světlo odrazí ve směru k zaostřovací čočce, za níž se nachází CCD (charge-coupled device) nebo CMOS (complementary metal-oxide semiconductor) obrazové filtry. Ty převádí světelné paprsky do elektronické podoby a za pomoci počítačového programu je sestrojen výsledný obraz otisku prstu.



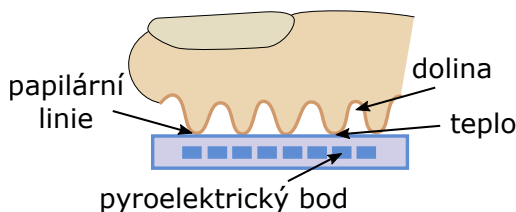
Obrázek 2.5: Schéma optického senzoru.

2. **Kapacitní senzory** (angl. capacitive sensors) jsou dnes zřejmě nejpoužívanějšími senzory, které se rychle rozvíjí, především v oblasti použití pro mobilní telefony. V tomto případě se otisk prstu přikládá k povrchu tvořeném skupinou mikrokondenzátorů. V momentě, kdy se prst dotkne tohoto povrchu, je vytvořen slabý elektrický náboj mezi bodem dotyku a povrchem senzoru. Tyto elektrické náboje jsou poté nosiči informací o výskytu papilárních linií. Tyto senzory mají menší plochu výsledného obrazu a ve srovnání s optickými senzory mají menší rozlišení a vyšší pořizovací cenu. Oproti optickým sensorům však fungují pouze po přiložení skutečného prstu lidské osoby, tedy žádný umělý materiál, tisk prstu na 3D tiskárně a jiné způsoby zfalšování u tohoto senzoru nemají šanci.



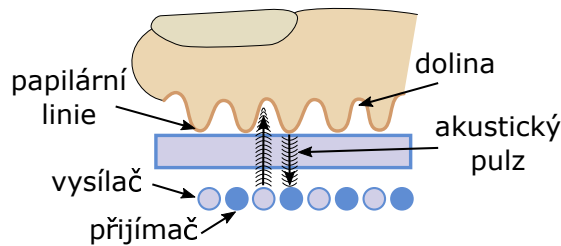
Obrázek 2.6: Schéma kapacitního senzoru.

3. **Tepelné senzory** (angl. thermal sensors) jsou tvořeny malými destičkami z pyroelektrického materiálu, které jsou velice citlivé na teplo. Přiložením prstu k těmto ploškám dojde v místě dotyku s povrchem k tepelné výměně. Tento rozdíl teplot je rozpoznán a následně na jeho základě zpracován obraz otisku prstu. Tento princip vyžaduje vyšší spotřebu energie a zároveň nepořizuje tak kvalitní obrazy otisku prstu jako jiné senzory. Navíc naráží na problém při teplých letních dnech, kdy rozdíl teploty okolního vzduchu a povrchu prstu není tak markantní.



Obrázek 2.7: Schéma tepelného senzoru.

4. **Ultrazvukové senzory** (angl. ultrasound sensors) jsou pravděpodobně nejnovější technologie použití senzoru otisku prstu. Pod povrchem senzoru se nachází dvě komponenty, a to vysílač akustických pulzů a jejich přijímač. Bylo zjištěno, že vrcholky papilárních linií mají ve srovnání s dolinou různou akustickou impedanci, a tak se vyslaný signál odrazí zpět k přijímači po uplynutí delší doby. Tímto je rozpoznána poloha papilárních linií a dolin. Tyto senzory se pyšní zatím nejvyšší úrovní zabezpečení. Jejich cena je bohužel mnohem vyšší.



Obrázek 2.8: Schéma ultrazvukového senzoru.

2.2 Zákonné povinnosti systému

Ze zákona vyplývá pro docházkové systémy několik implementačních povinností. V této kapitole budou zmíněny všechny poznatky, které je potřeba mít při tvorbě docházkového systému na paměti. Citace ze Záköníku práce (předpis č. 262/2006 Sb.) udává následující. [11]

§88 Přestávka v práci a bezpečnostní přestávka

1. Zaměstnavatel je povinen poskytnout zaměstnanci nejdéle po 6 hodinách nepřetržité práce přestávku v práci na jídlo a oddech v trvání nejméně 30 minut; mladistvému zaměstnanci musí být tato přestávka poskytnuta nejdéle po 4,5 hodinách nepřetržité práce. Jde-li o práce, které nemohou být přerušeny, musí být zaměstnanci i bez přerušování provozu nebo práce zajištěna přiměřená doba na oddech a jídlo; tato doba se započítává do pracovní doby. Mladistvému zaměstnanci musí vždy být poskytnuta přestávka na jídlo a oddech podle věty první.
2. Byla-li přestávka v práci na jídlo a oddech rozdělena, musí alespoň jedna její část činit nejméně 15 minut.
3. Přestávky v práci na jídlo a oddech se neposkytují na začátku a konci pracovní doby.
4. Poskytnuté přestávky v práci na jídlo a oddech se nezapočítávají do pracovní doby.

§90 Nepřetržitý odpočinek mezi dvěma směny

Zaměstnavatel je povinen rozvrhnout pracovní dobu tak, aby zaměstnanec měl mezi koncem jedné směny a začátkem následující směny nepřetržitý odpočinek po dobu alespoň 11 hodin, zaměstnanec mladší 18 let po dobu alespoň 12 hodin během 24 hodin po sobě jdoucích.

§96 Společná ustanovení o pracovní době a době odpočinku.

1. Zaměstnavatel je povinen vést u jednotlivých zaměstnanců evidenci s vyznačením začátku a konce
 - (a) odpracované
 - i. směny [§ 78 odst. 1 písm. c)],
 - ii. práce přesčas [§ 78 odst. 1 písm. i) a § 93],
 - iii. další dohodnuté práce přesčas (§ 93a),
 - iv. noční práce (§ 94),

- v. doby v době pracovní pohotovosti (§ 95 odst. 2),
(b) pracovní pohotovosti, kterou zaměstnanec držel [§ 78 odst. 1 písm. h) a § 95].

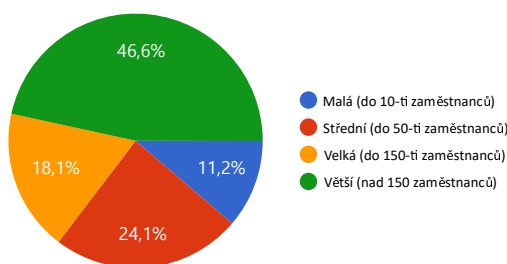
2. Na žádost zaměstnance je zaměstnavatel povinen umožnit zaměstnanci nahlédnout do jeho účtu pracovní doby nebo evidence pracovní doby a do jeho účtu mzdy a pořizovat si z nich výpisy, popřípadě stejnopisy na náklady zaměstnavatele.

2.3 Srovnání používaných systémů

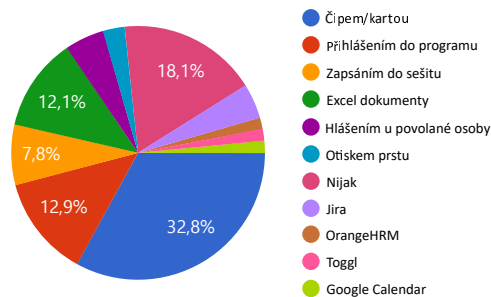
V praxi se můžeme především u velkých korporátních firem setkat s vlastními docházkovými systémy, které danou problematiku zápisu docházky řeší. U menších podniků je často k vidění použití veřejně nabízených docházkových systémů nebo třeba i kompletní absence docházkového systému. Avšak podle výsledků dotazníku spokojenosti, jenž byl na základě této bakalářské práce vypracován, a na který odpověděly téměř dvě stovky zaměstnanců, není práce s docházkovými systémy ve velkých firmách jednoduchá a nefunguje vždy tak, jak by si ji zaměstnanci představovali. Lidé si nejvíce stěžovali na nedostatečnou funkcionalitu, nízkou provázanost a v neposlední řadě chybovost používaných systémů. Ve výjimečných případech se objevilo, že zaměstnanci musí používat několik různých systémů, kde každý ze systémů řeší určitou oblast správy docházky.

Toto srovnávání používaných docházkových systémů je založeno na výsledcích dotazníku, který vyplnilo 197 lidí v okolí města Brna ve dnech od 20.11.2019 do 15.1.2020.

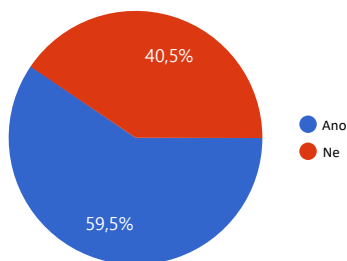
V úvodních částech dotazníku byli lidé vyzváni, aby zařadili společnost, ve které pracují, do skupiny podle množství zaměstnanců. Graf 2.9 ukazuje, že téměř polovina dotázaných pracuje ve velkých firmách čítajících více než 150 zaměstnanců. Nejvíce se ve firmách objevuje přihlašování pomocí čipu nebo karty. Pojednává o tom graf 2.10, kde si můžeme všimnout, že použití hesla je na druhém místě, a pouhých 2.5 % z dotázaných používá ve svém zaměstnání přihlášení za pomoci otisku prstu. Ze všech dotázaných nemá k docházkovému systému přístup téměř 40 % zaměstnanců, čímž se rozumí i úplná absence funkčnosti nahlédnutí na odpracovaný počet hodin. Z těch, jež k takovému systému přístup mají, je pouze 71 % spokojeno s jeho funkčností a možnostmi.



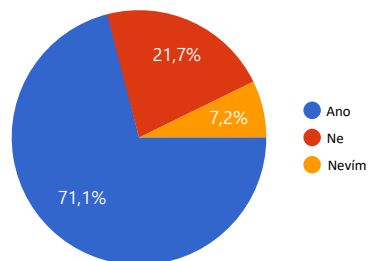
Obrázek 2.9: Rozdělení velikosti společnosti dotázaných zaměstnanců.



Obrázek 2.10: Způsoby přihlašování zaměstnanců.



Obrázek 2.11: Existence docházkového systému dotázaných.



Obrázek 2.12: Spokojenost dotázaných s jejich docházkovými systémy.

Na trhu existuje omezené množství systémů řešících problematiku docházky a správy zaměstnanců. Zde je uveden výběr těch, jež se objevili v dotazníku.

Jira a BambooHR

Jedná se o kombinaci dvou systémů, kde každý ze systémů částečně řeší problematiku docházkových systémů. Jira spadá pod firmu Atlassian, která má ústřednu v Austrálii, a BambooHR sídlí ve Spojených státech amerických. Zatímco první ze systémů se více zaměřuje na řízení projektů a pomáhá při jejich vývoji, tak BambooHR se zabývá databází zaměstnanců a jejich přehledem. Uživatelé těchto systémů se obvykle přihlašují do práce prostřednictvím přihlášení do systému Jira, kde mají pod svým účtem vedený projekt, na kterém aktuálně pracují. [7, 8]

OrangeHRM

OrangeHRM je velice rozšířený systém, původem z Ameriky, který v sobě zahrnuje velké množství modulů řešících různé oblasti problematiky docházkových systémů. K těmto modulům patří například:

- Management informací personálu - centrální databáze dat zaměstnanců a správy firmy.
- Management docházky - trekovací systém pro zaznamenání času.
- Systémová administrace - kontrola a nastavení funkcí.

Tento systém používají velké firmy jako je například Red Hat, Nasa a další. [9]

Toggl

Opět se jedná celosvětově rozšířený systém. Používají jej giganti jako je Google, Amazon nebo Github. Toggl se v hlavní řadě zabývá záznamem času a řazením úkolů mezi zaměstnanci. V základu nabízí 3 různé programy, které se liší dostupnými funkcemi a cenou, začínající od \$10 za zaměstnance měsíčně. [10]

Kapitola 3

Návrh systému

Docházkový systém bude tvořit webové rozhraní na straně klienta komunikující s aplikací na serveru pomocí asynchronní HTTP komunikace. Tato aplikace na straně serveru slouží jako prostředník pro komunikaci mezi uživatelem a databází. Přijímá tedy zprávy od uživatele, přistupuje k datům uloženým v databázi a následně uživateli vrátí odpověď na požadavek. V tomto modelu je serverová aplikace jediným modulem, který může komunikovat s databází, a je tedy zodpovědná za čtení i zápis dat.

3.1 Základní komponenty systému

V této sekci je popsána navržená funkčnost komplexnějších součástí systému.

Směny a záznamy

Systém k zapisování časových záznamů všech akcí pro jednotlivé zaměstnance využívá směny a záznamy. Směna je hlavní entitou, kterou lze přesně identifikovat pomocí data a identifikátoru zaměstnance. Každý zaměstnanec má tedy právě jednu směnu pro každý den a tato směna je automaticky generována na začátku každého dne pro všechny aktivní zaměstnance. Nese informace o aktuálním datu, identifikátoru zaměstnance a jeho fondu pro určitý den v týdnu. Zaměstnanec pak vytváří jednotlivé záznamy, které se k této směně vztahují. Záznam může nabývat jednoho z pěti možných typů, kterými jsou práce, oběd, pracovní cesta, pauza a home-office. Dále pak obsahuje časový záznam začátku a konce záznamu. Zaměstnanec může během jedné směny vytvořit neomezený počet záznamů, musí však být právě takového typu, který je pro zaměstnance v daný moment povolený. Například nelze vytvořit záznam pauzy, nemá-li otevřený záznam práce. Na obrázku 3.1 je možno vidět všechny povolené kombinace otevření a uzavření různých typů záznamů.

Směna v sobě také drží hodnotu odpracovaného času, která je aktualizována pokaždé, když zaměstnanec ukončí záznam typu práce, pracovní cesta nebo home-office. V takovém momentě je spočítán odpracovaný čas během tohoto záznamu včetně odečtení všech přestávek od začátku záznamu. Tento čas se projeví na hodnotě přesčasu daného zaměstnance. Směna však zůstává i nadále aktivní a zaměstnanec může například po ukončení svého záznamu práce zahájit záznam nový.

Na konci dne se automaticky uzavírají všechny směny. Zaměstnancům, kteří během dne nevytvořili žádný záznam práce, pracovní cesty nebo home-office, je odečten fond této směny od jejich hodnoty napracovaného přesčasu. Naopak těm zaměstnancům, kteří mají neukončený záznam a zároveň nemají povolení nočních směn, je automaticky záznam ukončen a

zapsána poznámka upozorňující na tuto událost. Pokud však povolení nočních směn mají, pak jsou jim záznamy pro aktuální směnu ukončeny a obratem znovu zapsány ve směně nové. Zároveň se zaměstnancům pracujícím déle než 6 hodin v kuse, mající obědovou pauzu kratší než 30 minut, odečte rozdíl jejich obědové pauzy od povinné přestávky trvající 30 minut a od celkově odpracovaného času. Systém zároveň vytvoří poznámku poukazující na tuto skutečnost.

Typ naposledy otevřeného záznamu	Lze začít záznam typu	Lze ukončit záznam typu
	práce, pracovní cesta, home-office	
práce	oběd, pracovní cesta, pauza	práce
oběd		oběd
pracovní cesta	oběd, pauza	pracovní cesta
pauza		pauza
home-office	oběd, pauza	home-office

Obrázek 3.1: Priorita záznamů.

Úprava a export záznamů

Zaměstnanec s právy personalisty může vytvořit, upravit nebo odstranit směny a záznamy. Rozhraní pro tuto úpravu zobrazí směny z posledních 30 dní. Pomocí filtrování podle data hodnotami od - do lze zobrazit libovolné množství záznamů od počátku systému až po dnešní den včetně. Všechny zobrazené hodnoty mohou být upraveny. Když je personalista s úpravami hodnot hotov, tak se mu po zvolené možnosti 'Uložit změny' zobrazí kontrolní soupis s informacemi o všech změnách které provedl, včetně hodnoty přesčasu ovlivněné těmito změnami. Personalista si může zkontrolovat platnost všech změn a rozhodnout se, zda-li se projeví změna přesčasu zaměstnance či nikoliv. Systém automaticky kontroluje všechny změny provedené uživatelem a pomáhá mu s korekcí dat kontrolními výpočty. Pokud tedy personalista změni příchod do práce, automaticky se změni odpracovaný čas.

Při úpravě směny je možno změnit hodnoty odpracovaného času, fondu a poznámky, nebo je další možností úplné odstranění směny. U záznamu je pak možno měnit hodnoty typu záznamu, jeho začátek, konec a poznámku, nebo odstranit celý záznam. Při vytváření směny je navíc možno zadat datum směny. Toto datum musí být platné a pro daného zaměstnance zatím neexistující. Systém k takto vytvořené směně doplní fond podle údajů z profilu zaměstnance pro konkrétní den v týdnu.

Právě zobrazené záznamy lze exportovat zvolením možnosti 'Export dat'. Exportování je možné provést do dvou různých formátů, a to buď PDF (angl. zkratka pro Portable Document File) nebo CSV (angl. zkratka pro Comma Separated Value), který je podporovaný například programem Microsoft Excel. V případě zvolení první možnosti PDF se záznamy zobrazí v novém panelu webového prohlížeče. Takto zobrazené záznamy jsou připraveny pro tisk nebo uložení na disk ve zmíněném formátu PDF. Druhá možnost exportování vytvoří soubor požadovaného formátu a uživateli odešle výzvu k jeho stažení.

Terminál

Terminálem se rozumí část rozhraní, která slouží zaměstnancům pro vykonávání akcí "Vytvoření nového záznamu" a "Ukončení existujícího záznamu". Očekává se, že toto rozhraní

bude k dispozici na specifickém zařízení (případně skupině zařízení) ve firmě, ke kterému budou mít zaměstnanci přístup a budou moci jednoduše vytvořit záznam, například o příchodu do práce. Pro správu zařízení, která zobrazují toto rozhraní, existuje služba v administrátorském panelu. Administrátor vyplní IP adresu požadovaného zařízení, a poté je možné přistoupit k terminálu na adrese [URL serveru]/terminal. Tímto je docíleno toho, že specifická zařízení mají přístup k terminálu i bez nutnosti přihlášení do systému (a prokázáním patřičných oprávnění), zatímco běžný uživatel se k terminálu nedostane.

Zaměstnanec však může načíst rozhraní terminálu v případě, že k tomu má speciální povolení, které uděluje personalista. Toto povolení se používá v případech, kdy zaměstnanec pracuje z domu nebo je například na dlouhé pracovní cestě. Terminál se zobrazí stejně, jako je tomu na zařízení s povolenou IP adresou a může vytvořit nebo ukončit jakýkoliv záznam.

Dovolená

O dovolenou žádá zaměstnanec prostřednictvím kalendáře, ve kterém si vybírá dny k uplatnění dovolené. Zaměstnanec si může zvolit buď celý den nebo jen půlku dne. Po odeslání žádosti o dovolenou musí počkat na její schválení nebo může žádost zrušit. Schvalování dovolené provádí vždy vedoucí a dovolenou může buď potvrdit nebo zamítnout.

Zaměstnanec při žádosti o dovolenou musí mít dostatečný počet dovolené k čerpání. Tato hodnota se odvíjí od celkového počtu dní dovolené za rok nastaveného pravidly firmy. Pokud tedy firma poskytuje 20 dní dovolené ročně a zaměstnanec je přijat na konci června, pak mu zbývá právě 10 dní dovolené do konce roku. Hodnota dovolené k čerpání se na začátku každého roku zvedne o hodnotu celkového počtu dní dovolené za rok. V případě že vedoucí zaměstnanci zamítne dovolenou, tak je zaměstnanci navrácen plný počet dní dovolené, o kterou žádal.

V den dovolené je zaměstnanec odlišen v seznamu zaměstnanců specifickou barvou. Pro tento den je mu vytvořena směna s fondem 0 hodin nebo polovinou jeho předpokládaného úvazku v případě, že zaměstnanec čerpá půl dne dovolené. V obou výše zmíněných případech však může přijít do práce a vytvořit nový záznam, jako kterýkoliv jiný den.

Státní svátky

V den státního svátku je všem zaměstnancům vytvořena směna s úvazkem na 0 hodin. Obdobně jako tomu je u dovolené, tak i zde může zaměstnanec vytvořit jakýkoliv záznam. Seznam státních svátků spravuje personalista, který v sekci "Správa svátků" může vytvořit, upravit nebo odstranit svátek. K dispozici je i možnost nahrání všech státních svátků pro zadaný rok z databáze svátků. Každý zaměstnanec pak ve svém kalendáři vidí všechny státní svátky včetně jejich popisku.

Automatické akce

V systému existují celkem tři akce, které se opakovaně provádějí v nastavený čas. Tyto akce kontrolují a spravují směny a záznamy zaměstnanců.

První akcí je kontrola správnosti vytvořených směn aktivních zaměstnanců. Při každém zapnutí systému se zkontroluje, zda-li pro dnešní den již byly vygenerovány směny aktivním zaměstnancům či nikoliv. Pokud tedy server v momentě generování nových směn neběžel (například vlivem výpadku), pak se při zapnutí systému všechny směny automaticky vygenerují a zaměstnanci se budou moci přihlásit do práce.

Druhá akce se provádí každý den ve 23:59 a slouží k ukončení otevřených záznamů aktivních zaměstnanců a případnému zapsání obědové pauzy. Pokud má zaměstnanec povolené noční směny a má neukončený záznam, pak je odhlášen s poznámkou o opětovném přihlášení do práce v momentě generování nové směny.

Poslední akce vytváří nové směny. Přesně v 00:01 se všem aktivním zaměstnancům vygeneruje nová směna s hodnotou fondu odpovídajícím jejich úvazku pro konkrétní den v týdnu. Pokud existuje poznámka o běžící noční směně zaměstnance, pak je automaticky vytvořen požadovaný záznam.

Správa hesel

Každý uživatel vlastní dvě různá hesla, jedno z nich označeno jako PIN (angl. zkratka slov Personal Identification Number). Tento PIN je používán při vytváření záznamů v rozhraní terminálu, zatímco druhé heslo zaměstnanec používá při přihlašování do systému. Zaměstnanec si tak může vytvořit jednodušší a rychlejší PIN a vyhnout se psaní jeho obvyklého hesla před ostatními zaměstnanci v prostoru terminálu. Zároveň je toto rozdělení výhodné zejména pro uživatele, kteří používají správce hesel, jako je například LastPass.

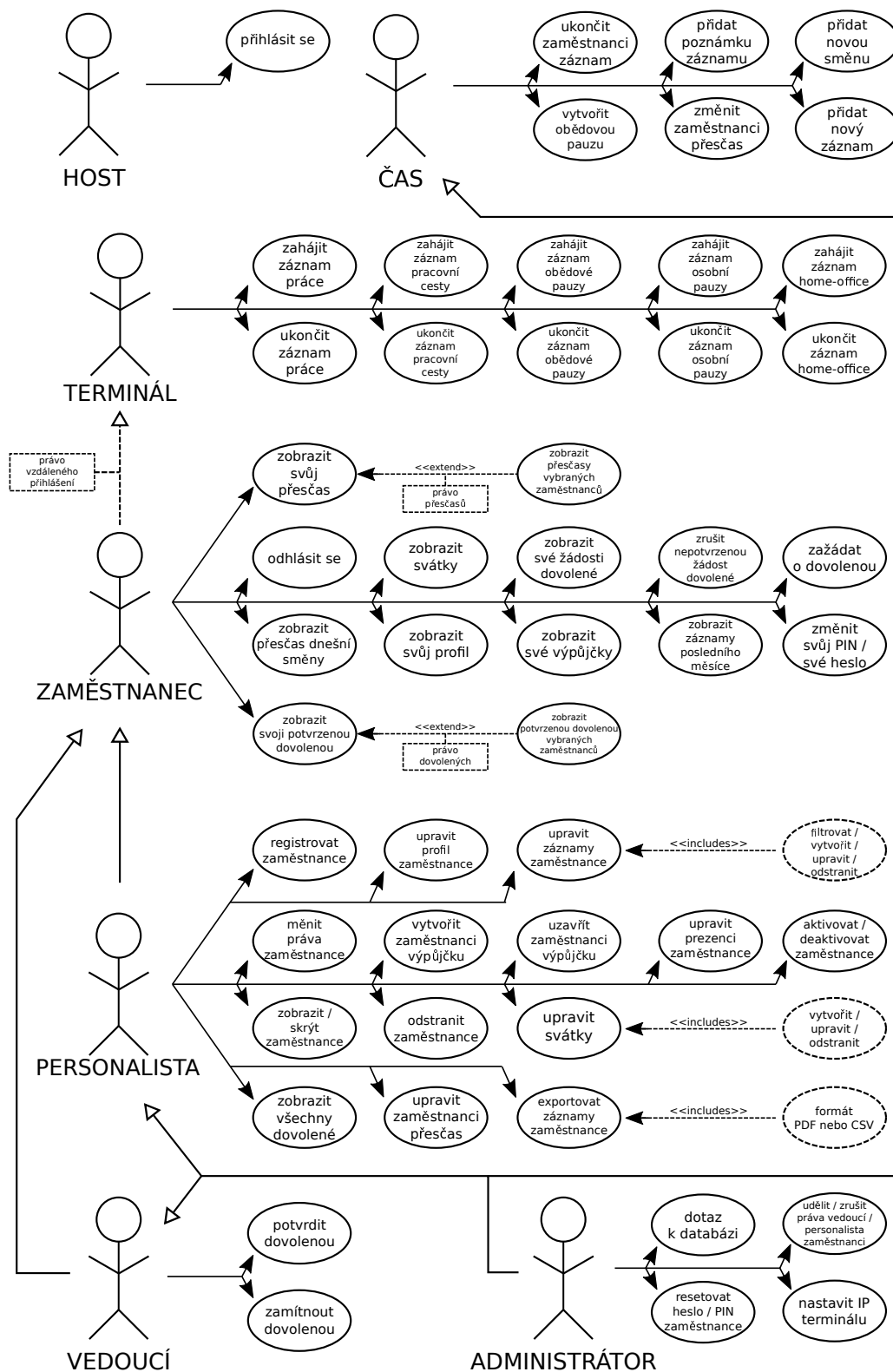
Každému nově registrovanému uživateli je nastaveno výchozí heslo na znak 'x' a PIN na číslici 1. Sám si pak v soukromí může tyto údaje změnit v sekci se svým profilem.

V případě zapomenutého hesla či PINu je administrátor schopen resetovat oba tyto údaje na výchozí hodnoty 'x' a 1.

3.2 Uživatelské role

Každý uživatel systému zastupuje při provádění akce určitou rolí. Tyto role nám určují především množinu operací, které může uživatel provádět, nebo naopak které jsou mu zakázány. K souhrnnému popsání všech rolí a jím povolených operací slouží diagram případů užití zobrazený na obrázku [3.2](#).

3.2.1 Diagram případů užití



Obrázek 3.2: Diagram případů použití.

V tomto diagramu si můžeme všimnout, že existuje celkem 7 různých rolí a každá z nich má v systému definované akce, které může provádět.

Host

Host je uživatelem systému, který není přihlášen. Jedná se tedy o návštěvníka, jehož jedinou možnou akcí je přihlášení. Bez úspěšné autorizace mu nejsou zobrazena žádná data. Návštěvník se do systému přihlásí kombinací platného uživatelského jména a hesla.

Zaměstnanec

Zaměstnancem se stává každý uživatel systému po úspěšném přihlášení. Každý zaměstnanec může zobrazit nadcházející státní svátky včetně poznámky, zobrazit informace o svém profilu, zobrazit své existující výpůjčky, změnit si heslo nebo PIN, zobrazit svůj přehled dovolené, vytvořit žádost o dovolenou, zrušit nepotvrzenou žádost o dovolenou, zobrazit svůj přesčas, podívat se na informace o dnešní směně, zobrazit své záznamy za poslední měsíc a odhlásit se ze systému.

Pokud má navíc práva na zobrazení přesčasů viditelných zaměstnanců, pak může zobrazit přesčasy všech uživatelů ve skupině viditelných zaměstnanců. Obdobně pokud má práva na zobrazení potvrzené dovolené, tak může vidět potvrzenou dovolenou ostatních zaměstnanců v téže skupině. V případě, že zaměstnanec má povolené právo pro vzdálené přihlášení, tak může využívat všech akcí, které poskytuje role terminálu.

Personalista

Jedná se o zaměstnance, který má speciální práva personalisty. Personalista automaticky nabývá všech akcí, které má zaměstnanec. Může ale navíc provádět akce jako registrování nového zaměstnance, úprava profilu zaměstnance, úprava, filtrování, vytváření a mazání záznamů a směn, dále může upravit práva zaměstnance, vytvořit novou nebo uzavřít již existující výpůjčku, upravit prezenci zaměstnance, přiřadit nebo odstranit zaměstnance ze skupin aktivních a viditelných uživatelů, upravit zaměstnanci přesčas nebo smazat celý profil zaměstnance. Personalista má práva vytvářet, upravovat a mazat svátky v systému, zobrazit všechny dovolené včetně zobrazení všech žádostí o dovolenou a exportovat filtrované záznamy uživatele do vybraných formátů.

Práva personalisty nastavuje administrátor systému. Personalista se sám nemůže vzdát těchto práv stejně tak jako předat tato práva jinému zaměstnanci.

Vedoucí

Vedoucím se stává zaměstnanec, který má aktivovaná práva vedoucího. Stejně jako tomu je u personalisty, tak i vedoucí může provádět všechny akce, které jsou definované pro klasického zaměstnance. Mimo tyto akce má právo na potvrzení nebo zamítnutí dovolené, o kterou zaměstnanec požádal.

Administrátor

Administrátor má vůbec největší práva v celém systému. Dohromady zaobaluje práva všech ostatních účastníků systému a navíc může resetovat heslo nebo PIN libovolnému uživateli na výchozí hodnoty, nastavit IP adresu zařízení pro zobrazení rozhraní terminálu a přistupovat

k databázi prostřednictvím dotazů typu SQL. Navíc může udělit nebo zrušit jak práva personalisty, tak práva vedoucího.

Terminál

Terminál obsahuje rozhraní pro vytváření nových záznamů nebo ukončení již existujících. Tuto roli zastupují zařízení, jejichž IP adresa je administrátorem zadána do seznamu IP adres terminálu. Také ji však může zastupovat zaměstnanec se zvláštním právem pro vzdálené přihlášení.

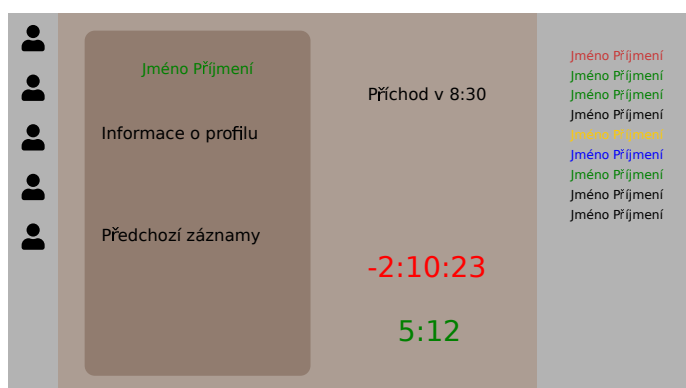
Čas

Čas do systému vnáší akce, které systém provádí automaticky v předem definovaném čase. K těmto akcím patří ukončení existujícího nebo vytvoření nového záznamu zaměstnance, přidání poznámky k záznamu či směně, vytvoření nové směny a změna přesčasu zaměstnance.

3.3 Grafické rozhraní

Při návrhu grafického rozhraní byl brán zřetel na intuitivní prostředí a maximální jednoduchost ovládání. Design se drží moderních trendů webových aplikací a využívá rozšířené používaných nástrojů pro práci s webovými stránkami, jako je například knihovna Bootstrap. Rozhraní je plně responzivní a dokáže se přizpůsobit jakémukoliv zařízení s šířkou displeje alespoň 350 pixelů.

Rozhraní zahrnuje široký sloupec v pravé části obrazovky obsahující seznam viditelných zaměstnanců ve firmě a v případě patřičných práv i informací o jejich docházce. Tento seznam používá barevné označení jmen jednotlivých zaměstnanců k vyjádření jejich přítomnosti nebo absence ve firmě. V levé části se nachází tenký vertikální pás jednoúrovňového menu s maximálně šesti položkami v závislosti na právech přihlášeného zaměstnance. Sloupec s docházkou ani menu po načtení stránky nemění a jejich obsah zůstává až na podbarvení stejný. Jednotlivé sekce se zobrazují v prostoru uprostřed mezi těmito sloupci a jejich obsah je měněn dynamicky bez nutnosti načítání celého webu.



Obrázek 3.3: Návrh grafického rozhraní.

Kapitola 4

Implementace

4.1 Použité technologie

Docker

Jedná se o moderní Open-Source aplikaci umožňující tzv. odlehčenou virtualizaci za účelem poskytnutí jednotného rozhraní pro izolaci aplikací do kontejnerů. Tato odlehčená virtualizace vytváří pouze virtuální obraz souborů potřebných pro fungování určitého prostředí (ne celého operačního systému, jak je tomu u virtualizace zvykem). Tím je docíleno velkého snížení režie a zároveň zaručení kompatibility na jakémkoliv stroji.

V tomto docházkovém systému bude Docker poskytovat virtualizaci prostředí pro běh databáze a serverové aplikace. Tyto dva obrazy je Docker schopen stáhnout ze svých vlastních serverů v předem zvolené verzi a současně pak obě prostředí spustit naprosto odděleně od ostatních aplikací běžících na serveru a nakonfigurovat spuštěná prostředí podle nastavení zapsaných v souboru docker-compose.json. Pro stažení konkrétních obrazů a konfiguraci kontejneru je využívá komponenta Docker-compose, která představuje vyšší úroveň abstrakce nad Dockerem. Pomocí jednoduchého zápisu v jediném souboru je nastaveno mapování vnitřních a vnějších portů kontejneru, úložisté pro ukládání dat a spouštění serverů NodeJs a MySQL.

MySQL databáze

Server MySQL běží ve verzi 8 a pro komunikaci se serverem NodeJs používá port 3306, který se běžně používá pro komunikaci s MySQL. Po prvním spuštění serveru MySQL jsou automaticky provedeny SQL příkazy v souborech init.sql a root.sql. Soubor init.sql obsahuje celou strukturu databáze a vytváří všechny tabulky včetně jejich vzájemných vztahů a sloupců. Root.sql pak slouží k vytvoření administrátorského účtu s uživatelským jménem "admin" a výchozím heslem "x".

NodeJs

NodeJS je běhové prostředí pro jazyk JavaScript. Ten bylo možno vždy vykonávat pouze pod záštitou webového prohlížeče (například Google Chrome), který obsahoval jádro potřebné pro provádění příkazů tohoto jazyku. Právě z tohoto důvodu bylo možné mít aplikaci spuštěnou pouze na straně klienta, nikoli serveru. S moderním nástrojem NodeJS, který zahrnuje jádro pohánějící JavaScript z prohlížeče Google Chrome, je tento problém odbourán a webový prohlížeč již není nutnou součástí javascriptového kódu. Využití tohoto řešení při-

nášší velkou spoustu výhod, mezi nimiž je nejdůležitější, že NodeJs provádí všechny akce asynchronně. Díky tomuto dokáže jeden proces obsluhovat velké množství uživatelů, protože místo čekání na vyřízení dotazu se již věnuje jinému klientovi.

Díky správci balíčků pro JavaScript (angl. Node Package Manager nebo NPM) je jednoduché vybrat si a využít balíček z velkého množství knihoven, které nabízejí jednoduchá řešení častých problémů při vývoji webové aplikace. Tyto balíčky jsou staženy ze serveru podle předpisu v souboru package.json. Všechny stažené balíčky jsou pak k dispozici v adresáři *node_modules*. Při implementaci této práce byly použity následující balíčky:

- **body-parser** slouží k parsování příchozích dat. Díky tomuto balíčku je možno pracovat s příchozími daty jako s objekty.
- **csv-writer** pomáhá s vytvářením souborů typu CSV. Objekt třídy CsvWriter se inicializuje parametry pro cestu k souboru a hlavičkou, která drží informace o jednotlivých sloupcích. Poté se použitím metody writeRecords zapíše data do souboru. Tento formát se používá při exportu záznamů zaměstnance.
- **date-holidays** je balíček, který obsahuje databázi státních svátků pro 144 zemí. Personalista může využít této databáze při hromadném nahrání státních svátků do systému v sekci "Správa svátků".
- **ejs** je zkratkou pro Embedded JavaScript a používá se pro přímé vložení javascriptového kódu v html. Pomocí tohoto rozšíření HTML je možné provádět podmínky a smyčky, definovat vlastní proměnné a provádět výpočty nad daty které chceme zobrazit. Výsledné HTML se renderuje z EJS šablony metodou render. Tato šablona je použita pro vykreslení všech souborů HTML v celém systému.
- **express** zajišťuje samotné spuštění serveru včetně routování všech přístupných adres. Jedná se o nejrozšířenější balíček NodeJs, což potvrzuje i rekordní počet stahování, který průměrně každý týden překročí hranici 13 milionů.
- **express-session** je rozšířením balíčku express a slouží pro správu session. Pomáhá s jejím vytvořením, hashováním i přístupem.
- **moment** obsahuje rozsáhlé možnosti pro správu času. Vhod přijde při generování časových záznamů nebo jejich formátování či kontrole.
- **moment-timezone** rozšiřuje balíček moment o nastavení časové zóny a díky tomu může generovat čas i datum vždy přesně pro naše časové pásmo včetně přechodů letního a zimního času.
- **mysql** zjednodušuje připojení k MySQL databázi. Po konfiguraci lze vytvořit připojení použitím metody createConnection.
- **node-schedule** vytváří rozhraní pro automatické volání akcí v předem nastavený čas.
- **node-schedule-tz** přináší možnost balíčku node-schedule nastavit časovou zónu pro kontrolu času vykonání funkce. Po nastavení pracuje balíček s českým časem včetně přechodu letního a zimního času.
- **socket.io** je balíček, který slouží k posílání zpráv mezi klientem a serverem. Tyto zprávy mohou obsahovat i data ve formátu JSON. V této práci se však primárně pro

komunikaci klienta a serveru používá ajax. Hlavní využití balíčku sockets.io přichází s možností broadcastového posílání zprávy všem připojeným uživatelům. Díky tomu je možné okamžitě dát všem klientům vědět, když nějaký ze zaměstnanců provede například akci odchod z práce. Díky zprávě vyslané broadcastem se všem klientům změní označení daného zaměstnance.

Jquery

Jedná se o knihovnu JavaScriptu a přináší nám výhody v práci se stránkami na straně klienta. Dokáže obalit HTML DOM element a poté s ním provádět různé funkce měnící třídy a atributy elementu. Usnadňuje práci a odesílání formulářů a díky jednoduché syntaxi je kód mnohem čitelnější než v případě použití běžných funkcí JavaScriptu. Výhodou knihovny Jquery je i možnost jednodušší notace pro využití ajaxu. Ajax je zkratkou pro Asynchronous JavaScript and XML (Extensible Markup Language). Zprávy využívající ajax hrají v systému velkou roli, protože dokáží od klienta odeslat data serveru a s použitím JavaScript Promises zareagovat na odpověď od serveru bez nutnosti znovunačtení stránky ve webovém prohlížeči.

Bootstrap

Bootstrap je knihovnou pro CSS (Cascading Style Sheets) a JavaScript. Na rozdíl od Jquery, které je orientované pro práci s daty na pozadí klientského rozhraní, se Bootstrap zaměřuje na práci s grafickým rozhráním. Pomáhá se stylováním a vykreslením různých objektů a animací, které se ve webových aplikacích zobrazují. Využití této knihovny lze pozorovat při vyplňování formuláře nebo zobrazení modalového okna.

4.2 Kontejner

Kontejner je standardní jednotka softwaru, která obaluje kód a všechny jeho závislosti do jediného celku, který dokáže fungovat rychleji a především nezávisle na výpočetním prostředí. Obraz Docker kontejneru je lehký a samostatně spustitelný balíček softwaru, který obsahuje vše potřebné pro spuštění aplikace: kód, runtime, systémové nástroje, systémové knihovny a nastavení.

Kontejner se spouští pomocí souboru Makefile v kořenovém adresáři systému příkazem `make`. Obsahuje obrazy serveru MySQL pro databázi a NodeJs pro aplikaci. Oba dva obrazy startují současně, NodeJs je však pozastaven a čeká 30 vteřin na úspěšné spuštění obrazu MySQL, na kterém je závislý. Při prvním spuštění obrazu MySQL se vytváří databáze. Kontejner po spuštění běží na pozadí v tzv. detach módu, takže je nezávislý na terminálu. Zastavení kontejneru je možné provedením příkazu `make stop`. Pro přístup k logům jednotlivých obrazů lze využít příkazy `docker logs -f node` nebo `docker logs -f mysql`. K databázi se lze připojit příkazy `sudo docker exec -it mysql mysql -u root -px` a následně `use mysqlpdb`.

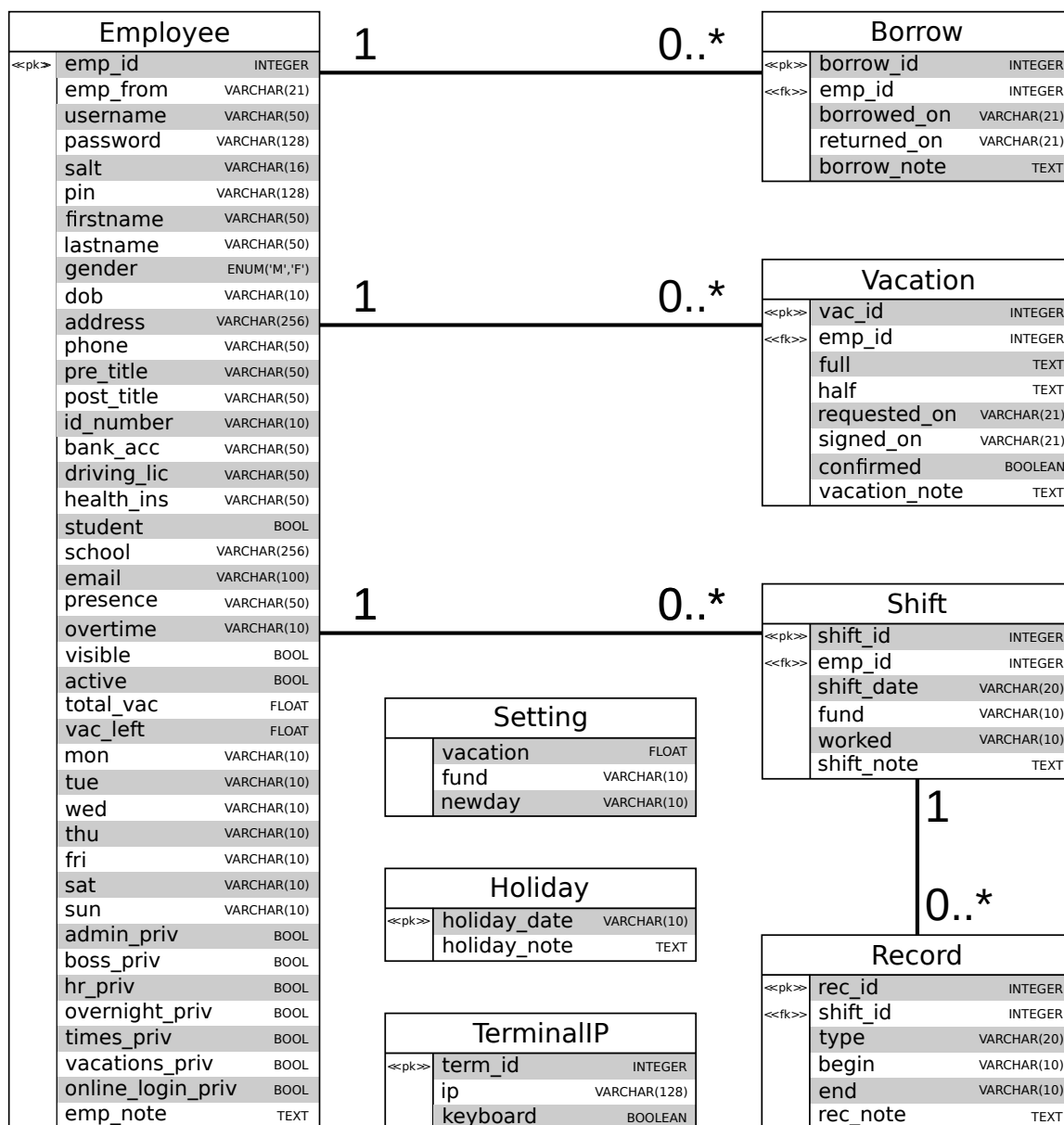
4.3 Databáze

Při výběru typu databáze pro implementaci docházkového systému bylo uvažováno mezi relačními a NoSQL databázemi. Největší výhodou databází typu NoSQL je rychlejší přístup k velkému objemu dat. Hlavním zástupcem této databáze je mongoDB, moderní a rychle

se rozvíjející databáze založená na principu ukládání souborů ve formátu nazvaném BSON, který je podobný notaci JSON. Na druhé straně, relační databáze řadí data do tabulek, které obsahují sloupce sloužící jako předpis pro data zapsaná v řádcích. Databáze nabízí možnost provázání jednotlivých tabulek a vytvoření vazeb, a právě díky těmto vazbám je relační databáze lepším kandidátem pro implementaci docházkového systému. Propojení dat zaměstnance s časovými záznamy jeho aktivit nabízí snadné a elegantní řešení. Z nabídky relačních databází byla zvolena databáze MySQL ve verzi 8.

Databáze slouží pro uchování všech dat docházkového systému a přístup k těmto datům má pouze serverová aplikace, která s databází komunikuje prostřednictvím dotazů na předem dohodnutém portu 3306. Komunikace probíhá dotazovacím jazykem SQL.

4.3.1 Model databáze



Obrázek 4.1: Model logického návrhu databáze.

Zaměstnanec

Základní entitou systému je uživatel, který je reprezentován tabulkou Zaměstnanec (angl. Employee). Tato tabulka používá unikátní identifikátor emp_id k rozpoznání specifického zaměstnance. Obsahuje všechny informace o jeho profilu včetně soli, hesla a pinu. Dále spravuje údaje o úvazku uživatele, jako je fond pro každý den v týdnu a počet dovolené. Mimo to drží hodnoty flagů pro všechna práva zaměstnance a řazení do skupin aktivních a viditelných zaměstnanců.

Výpůjčka

Výpůjčky slouží k zaznamenání údajů o zapůjčení předmětu zaměstnanci. Jsou uloženy v tabulce Výpůjčka (angl. Borrow). K identifikaci konkrétního záznamu se používá unikátní hodnota borrow_id. Mimo to se každá výpůjčka váže k zaměstnanci pomocí jeho identifikátoru emp_id a obsahuje datum vypůjčení, datum navrácení a poznámku. Se zaměstnancem je ve vztahu 1:N, tedy jednomu zaměstnanci může být přiděleno 0 až N výpůjček. V případě odstranění zaměstnance s identifikátorem, který se váže k některé z výpůjček, je odstraněna i celá výpůjčka.

Dovolená

Tabulka Dovolená (angl. Vacation) slouží k uchování záznamů a žádostí o dovolenou. Opět stejně jako výpůjčka má jedinečný identifikátor vac_id a váže se vždy k nějakému zaměstnanci. Dovolená obsahuje seznam dní a půlek dní, časovou značku vytvoření a rozhodnutí, vyjádření vedoucího a poznámku. Se zaměstnancem jsou opět ve vztahu 1:N, kde každý zaměstnanec může mít 0 až N záznamů dovolené.

Směna

Nové směny se automaticky generují systémem. Pro uchování těchto směn se používá tabulka Směna (angl. Shift). Ta obsahuje identifikátor směny a zaměstnance, pro kterého je směna generována, datum směny a odpracovanou dobu s fondem konkrétní směny a poznámku. Kardinalita vztahu s tabulkou Zaměstnanec je 1:N.

Záznam

Všechny záznamy, které uživatel vytvoří se ukládají v tabulce Záznam (angl. Record). Každý záznam lze identifikovat pomocí rec_id a vztahuje se ke směně. Vztah mezi směnou a záznamem je 1:N, jedna směna má N záznamů. Záznam je určen typem, začátkem a koncem a může obsahovat poznámku.

Nastavení

Tabulka nastavení (angl. Setting) vlastní tři sloupce, které slouží k základnímu nastavení systému. Tato tabulka jako jediná nemá žádný unikátní klíč. Data se do tabulky zapisují pouze při prvním vytvoření databáze. Vytvořen je pouze jeden řádek, a pak je možné pouze měnit existující hodnoty. Tabulka obsahuje sloupec vacation, který drží výchozí hodnotu počtu dovolené na rok pro nově registrujícího uživatele, sloupec fund definující výchozí hodnotu úvazku pro pracovní den a záznam newday, který má hodnotu data posledního generování nových směn. Toto datum se používá pro kontrolu při zapínání serveru.

Svátek

Všechny svátky v systému jsou realizovány tabulkou Svátků (angl. Holiday). V této tabulce je unikátním identifikátorem datum svátku. Není tedy povoleno mít na jeden den dva různé svátky. Pak zde nalezneme poznámku, která značí o jaký svátek se jedná.

IP terminálu

Anglicky TerminalIP je tabulka sloužící k uchování IP adres zařízení, které jsou určeny k zobrazení rozhraní terminálu. Tabulka obsahuje pouze identifikátor term_id a hodnotu samotné IP adresy. TerminalIP není ve vztahu s žádnou jinou tabulkou.

4.3.2 Záloha a obnovení dat

K zálohování databáze slouží utilita mysqldump. Ta dokáže vygenerovat sérii SQL příkazů na základě aktuálních dat uložených v databázi. Jedná se o kompletní zálohu databáze včetně databázových tabulek a datových typů jednotlivých sloupců. Zálohu je možné provést příkazem make backup v hlavním adresáři systému, kde se nachází soubor Makefile. Po provedení uvedeného příkazu se výsledné SQL příkazy uloží do souboru backup.sql. Obnovení databáze z vytvořené zálohy provede volání všech SQL příkazů v souboru vygenerovaném pomocí mysqldump. Příkazem make restore se nahradí současná databáze příkazy ze souboru backup.sql. Takto navrácená databáze přijde o všechny změny, které nastaly až po provedení zálohy.

4.4 Serverová aplikace

Jedná se o program v jazyce JavaScript, běžící na serverové stanici, který je spuštěn v běhovém prostředí NodeJs a jeho hlavní rolí je příjem zpráv od uživatele, jejich zpracování a následná odpověď uživateli. Tyto zprávy přichází asynchronně z různých stanic a reprezentují různé akce uživatele, například požadavek na zobrazení rozhraní. Hlavním souborem, který spouští server a nastavuje připojení k databázi a routování aplikace je soubor app.js. V adresářové struktuře lze nalézt složky views, public a js.

app.js

App.js je souborem, který se spouští při startu kontejneru NodeJs. V první řadě se nahrají všechny používané balíčky z adresáře node_modules a vytvoří se příslušné objekty, pak se vytváří připojení k databázi podle zvolené konfigurace a definují se funkce pro komunikaci s databází. Dále se nastavují časové akce, které vykonávají zvolenou funkci vždy v určitém čase. Následuje nastavení rozhraní, které zpřístupňuje adresář public uživatelům a nastavuje nástroj pro vykreslování obrazů ze složky views. Další částí je mapování funkcí ke všem podporovaným adresám systému. Nakonec probíhá samotné spuštění serveru a nastavení služby sockets.io pro posílání hromadných zpráv všem uživatelům naráz.

views

Adresář views obsahuje obrazy, pomocí kterých je vykreslováno grafické rozhraní. Soubory obsažené v této složce jsou formátu ejs a jedná se o HTML kód, který navíc obsahuje speciální značky, které umožňují vložit kód javascriptu. Některé ze souborů slouží k vykreslení celé stránky, jiné se používají pouze k zobrazení specifické sekce nebo zprávy.

public

Složka public je veřejným adresářem, ke kterému má přístup každý uživatel systému. Jsou zde obsaženy javascriptové kódy, které se spouští v prohlížeči na straně klienta, kaskádové

styly a soubory knihoven, jako je například Bootstrap nebo JQuery a obrázky použité v rozhraní terminálu. Všechny soubory knihoven jsou lokálně staženy a při vkládání do kódu se nepoužívají CDN (zkratka pro Content Delivery Network) odkazy z důvodu omezení počtu závislostí systému.

js

Adresář js obsahuje logiku serverové aplikace. Jednotlivé javascriptové soubory řeší část funkcionality. Soubor `authenticate.js` pomáhá s ověřením uživatele při přihlašování do systému, `passwords.js` obsahuje šifrovací metodu a nástroj pro generování soli, `queries.js` zase provádí všechny dotazy do databáze a `scheduler.js` definuje časové funkce. Nakonec `time.js` vytváří časové záznamy a formátuje čas i datum pro použití v celém systému. V podadresáři `routes` se nachází směrování pro jednotlivé aktéry docházkového systému. Aktéři se rozlišují podle pravomocí na `admina (admin)`, `personalistu (hr)`, `zaměstnance (employee)` a `nepřihlášeného uživatele (user)`. Dále pak směrování pro rozhraní terminálu (`terminal`) a nahrání menu včetně seznamu zaměstnanců je proveden souborem `index.js`.

4.5 Make

Make je nástroj, který umožňuje postupné vykonání jednotlivých úloh zapsaných v souboru `Makefile`. Provádí se příkazem `make` v kombinaci s klíčovým slovem daného příkazu. `Makefile` docházkového systému podporuje následující příkazy:

- `make` spouští celý kontejner a startuje obrazy MySQL a NodeJs.
- `make run` má stejnou funkčnost jako samotný příkaz `make`.
- `make runserver` spouští pouze obraz NodeJs. MySQL zůstává neaktivní.
- `make rundb` spouští pouze obraz MySQL. NodeJs zůstává neaktivní.
- `make stop` zastavuje spuštěný kontejner včetně všech běžících obrazů.
- `make cleanall` zastaví spuštěný kontejner včetně všech běžících obrazů a smaže všechna uložená data.
- `make backup` vytvoří zálohu databáze v souboru `backup.sql`.
- `make restore` nahraje databázi ze souboru `backup.sql`.

Kapitola 5

Testování

Testování aplikace probíhalo v několika fázích. Tou první bylo lokální testování všech komponent systému na operačních systémech Ubuntu verze 18.03. a Gentoo. Toto testování probíhalo souběžně s vývojem aplikace, a u každé nově přidané funkcionality bylo sledováno chování jak při zadání správného vstupu, tak při zadání nesmyslných hodnot a chybných stavů. Finální verze vývoje pak byly testovány na fakultním serveru a interním serveru IT firmy v Brně.

5.1 Nasazení na fakultním serveru

Docházkový systém byl nasazen na fakultním serveru `ant-build.fit.vutbr.cz`, na systému Debian GNU/Linux 10, Docker verze 18.09.1 a Docker-compose verze 1.21.0. Testování probíhalo po dobu více než dvou týdnů a v jeho průběhu byl vytvořen sedmidenní testovací plán, kterého se zúčastnilo 10 dobrovolníků. V této skupině se nacházeli jak lidé se specializací v oblasti informačních technologií, tak i zástupci přírodovědných a humanitárních oborů.

Testovací plán

1. Po vytvoření prázdné databáze je uživatelem admin vytvořen účet s právy personalisty pro zaměstnance A a účet s právy vedoucího pro zaměstnance B.
2. Zaměstnanec A postupně registruje dalších 8 zaměstnanců. Všem zaměstnancům nastaví 10 dní dovolené. Náhodně vybere dva zaměstnance a označí je jako studenty, název školy vybere ze seznamu vysokých škol v Brně. Osobní údaje všech registrovaných zaměstnanců vyplní dle vlastního uvážení a nastaví jim úvazky a práva následovně:
 - Zaměstnanci C, D, E mají osmi-hodinový úvazek pro všechny pracovní dny v týdnu a nejsou jim přidělena žádná práva s výjimkou práva pro vzdálené přihlášení. Tito zaměstnanci představují běžné uživatele docházkového systému s úvazkem na 40 hodin.
 - Zaměstnanec F má šesti-hodinový úvazek pro všechny pracovní dny v týdnu a vlastní práva pro zobrazení přesčasů ostatních zaměstnanců a právo pro vzdálené přihlášení.

- Zaměstnanec G má osmi-hodinový úvazek pro pondělí, sedmi-hodinový úvazek pro úterý a vlastní práva pro zobrazení přesčasů a dovolených ostatních zaměstnanců a právo pro vzdálené přihlášení.
 - Zaměstnanec H má šesti-hodinový úvazek pro každý den v týdnu včetně víkendu a vlastní práva pro zobrazení přesčasů a dovolených ostatních zaměstnanců, povolení nočních směn a právo pro vzdálené přihlášení.
 - Zaměstnanec I má různý úvazek pro každý den v týdnu včetně víkendu a vlastní práva pro zobrazení přesčasů a dovolených ostatních zaměstnanců, povolení nočních směn a právo pro vzdálené přihlášení.
 - Zaměstnanec J má nulový úvazek pro všechny dny v týdnu a nejsou mu přidělena žádná práva.
3. Všichni zaměstnanci si změni svá hesla a PIN.
 4. Zaměstnanci A - I jsou zobrazeni v přehledu a aktivováni. Zaměstnanec I je jako jediný aktivován okamžitě, ostatní s možností od zítřejšího dne.
 5. Všichni zaměstnanci poctivě plní docházku a využívají všech záznamů, které nabízí rozhraní terminálu (práce, pracovní cesta, oběd, pauza, home-office) dle vlastního uvážení.
 6. Zaměstnanci D, E, F žádají o dovolenou v následujících dnech. Využijí přitom možnost celého dne i poloviny.
 7. Zaměstnanec B potvrdí dovolenou zaměstnanci E, F a zamítne dovolenou zaměstnance D.
 8. Personalista vytváří všem zaměstnancům výpůjčky a sleduje záznamy dle vlastního uvážení.
 9. Zaměstnanci G a I se ve vybraný den neodhlásí z práce.
 10. Poslední den testování personalista uloží všechny záznamy zaměstnanců v obou nabízených formátech.

5.2 Nasazení v reálném prostředí

Docházkový systém byl za účelem testování nasazen v prostorech brněnské IT firmy s 20 zaměstnanci. Běžel na systému CentOS Linux 8 a o virtualizaci kontejneru se staral výchozí software distribuce CentOS, systém Podman. Podman je program vyvíjený skupinou vývojářů, kteří s jeho vývojem začali v momentě, kdy Docker změnil svá licenční práva. Podman je stále v ranné verzi vývoje a snaží se o maximální kompatibilitu se systémem Docker. Na testovacím serveru byl nainstalován Podman ve verzi 1.6.4 a Podman-compose v poslední dostupné verzi z větve devel ke dni 11.5.2020.

K nasazení docházkového systému v prostředí Podmanu bylo nutné poupravit příkazy volané ze souboru Makefile. Kompletní seznam změn byl následující:

- `docker-compose up node -> podman-compose up node`
- `docker-compose up mysql -> podman-compose up mysql`

- `docker-compose up -> podman-compose up`
- `docker-compose down -> podman-compose down`
- `docker-compose down -v || true -> podman-compose down -v || true`
- `docker exec mysql /usr/bin/mysqldump -u root -password=x mysqlpdb > backup.sql`
`-> podman exec mysql /usr/bin/mysqldump -u root -password=x mysqlpdb > backup.sql`
- `cat backup.sql | docker exec -i mysql /usr/bin/mysql -u root -password=x`
`mysqlpdb -> cat backup.sql | podman exec -i mysql /usr/bin/mysql -u root`
`-password=x mysqlpdb`

Do testování se zapojilo všech 20 zaměstnanců firmy včetně zkušené personalistky s mnohaletými zkušenostmi s prací v různých komerčních docházkových systémech. Na rozdíl od testování na fakultním přístroji, kde se zaměstnanci do práce přihlašovali pouze vzdáleně s příslušnými právy, v prostorách firmy bylo vyhrazeno zařízení sloužící jako terminál pro zadávání záznamů. Terminál byl umístěn v prostorech při vchodu do budovy a zaměstnanci mohli zaznamenávat časové údaje ihned při příchodu nebo těsně před odchodem z pracoviště.

5.3 Výsledky testování

Z online testování docházkového systému vyplynulo několik nedostatků. Docházkový systém používal pro komunikaci zprávy typu HTTP a webový prohlížeč z tohoto důvodu při vyplňování formuláře zobrazoval rozsáhlá varování. Proto byl server upraven, aby používal pouze zprávy typu HTTPS a byl přidán certifikát pro ověření webu. Certifikát nebyl podepsán certifikační autoritou, a tak je potřeba před přístupem k webu potvrdit výjimku pro daný web. Zároveň je v URL adrese nutné uvést `https://` před adresou serveru.

Testování na fakultním serveru odhalilo ojedinělé chyby v počítání přesčasů směn po zadání specifické kombinace záznamů. Tato chyba vznikla špatným zpracováním záznamů na straně serveru a byla okamžitě opravena. Dotázaní si pochvalovali grafické rozhraní a jednoduchost ovládání docházkového systému. Uvedli, že systém je přehledný a nevyskytly se problémy s pochopením funkcionality nebo hledáním položek jak na stolním počítači, tak při používání mobilního zařízení.

Při testování systému v reálném prostředí společnosti, která nepoužívá žádný komerční systém tento systém obdržel značně pozitivní ohlasy. Testování navíc probíhalo s využitím přihlašovacího terminálu, takže zaměstnancům nebylo nastaveno právo pro vzdálené přihlášení. Jako doporučené rozšíření k tomuto způsobu byla implementována virtuální klávesnice pro zadávání uživatelského jména a hesla na dotykové obrazovce. Aktivování klávesnice je možné provést v administrátorském panelu pouze pro terminály, které se zobrazují pomocí nastavené IP adresy a nelze ji tedy zobrazit u uživatele přihlašujícího se prostřednictvím svých práv pro vzdálené přihlášení. Zaměstnanci kladně hodnotili možnost vidět trvání aktuální směny v reálném čase a zobrazení aktivity všech zaměstnanců bez nutnosti obnovení stránky. Personálnímu oddělení naopak postrádalo funkce pro hromadné exportování zaměstnanců a rozsáhlejší hierarchii potvrzování dovolené. Uživatelé byli zpočátku zmateni existencí dvou hesel a jejich vzájemným používáním. Po prvním neúspěšném přihlášení v terminálu se však všichni rychle adaptovali a uvedli, že s následným používáním hesla a pinu již problémy neměli.

Kapitola 6

Závěr

Cílem této bakalářské práce bylo provést výzkum nejčastěji používaných metod pro identifikaci osob, prozkoumat konkurenční systémy docházkových systémů a vytvořit systém pro evidenci docházky zaměstnanců na pracovišti s možnostmi exportování časových záznamů jednotlivých zaměstnanců a rozhraním pro žádání a potvrzování dovolené.

Docházkový systém se povedlo implementovat dle zadání a rozhraní uživatelům tvoří webová aplikace, která umožňuje všem zaměstnancům zobrazit svůj vlastní přehled záznamů, dovolené a informací o svém profilu ve vlastním webovém prohlížeči na jakémkoliv zařízení, od telefonu až po stolní počítač. Stejně rozhraní slouží personalistům ke správě všech zaměstnanců a exportu jejich časových záznamů, vedoucím pak k potvrzení dovolené.

Systém byl úspěšně nasazen na fakultním stroji, kde za účelem testování běžel po dobu deseti dní. Zároveň byl spuštěn pro testovací účely i v reálném prostředí brněnské firmy s použitím virtualizace pomocí systému podman. Testování ojedinele odhalilo drobnější chyby, které byly v systému okamžitě opraveny. V obou případech testování systém obdržel kladná hodnocení od všech zúčastněných a jeho hlavní předností byla uvedena jednoduchost ovládání a přívětivý vzhled uživatelského rozhraní. Naopak v nedostacích systému se objevila absence rozšířené funkcionality v rozhraní personalisty a omezené možnosti správy dovolené.

6.1 Budoucí práce

Z výsledků testování vyplynulo, že tento docházkový systém je po odstranění zmíněných nedostatků plně konkurence schopný. Proto se v budoucí práci chystá rozšíření stávajícího systému o následující funkcionalitu:

- **Hromadné exportování záznamů** - Rozhraní pro personalistu, které umožňuje exportování záznamů z určitého rozmezí dat pro vybranou skupinu zaměstnanců na jednu pro zvolený formát.
- **Vyhledávač zaměstnance v přehledu zaměstnanců** - V seznamu všech zaměstnanců v rozhraní personalisty doplnit funkcionalitu pro vyhledání konkrétního zaměstnance.
- **Hierarchie potvrzování dovolené** - Vytvoření hierarchie při potvrzování dovolené. Pro každého zaměstnance je možno nastavit skupinu nadřízených, kteří budou mít práva k potvrzení nebo zamítnutí jeho žádostí o dovolenou. V případě že přímý nad-

řízený potvrdí zaměstnanci dovolenou, tak se požadavek přenesse na výše postaveného. Pokud některý ze článků dovolenou zamítne, tak je celá žádost zrušena.

- **Přidání nových záznamů** - Vytvoření nových typů záznamů pro návštěvu doktora, náhradní volno, pracovní volno, aj.
- **Posílání e-mailových zpráv** - Automaticky posílat e-mailová upozornění při aktivitě v systému. Příkladem může být e-mail vyzývající vedoucího k vyjádření k žádosti o dovolenou.
- **Automatické zálohování databáze** - Nastavení periodického zálohování databáze.
- **Automatické mazání vygenerovaných souborů** - Mazání souborů, které jsou vytvořeny v momentě exportování záznamů do formátu csv.

Literatura

- [1] Dostupné z: <https://blog.avast.com/hs-fs/hubfs/top-10-unsecure-passwords.jpg?width=265&name=top-10-unsecure-passwords.jpg>.
- [2] Dostupné z: https://cdn1-shop.mikroe.com/img/product/rfid-reader-board/rfid-reader-board-large_default-1.jpg.
- [3] Dostupné z: <https://5.imimg.com/data5/VN/YR/MY-3183350/rfid-chip-500x500.jpg>.
- [4] Dostupné z: <https://elainnovation.com/Local/ela/files/1126/bigSCIEL.READER.WF2.png>.
- [5] Dostupné z: https://www.researchgate.net/profile/Yassine_Naija/publication/330545779/figure/fig3/AS:717973031514113@1548189518502/Example-of-active-RFID-tag.jpg.
- [6] Dostupné z: <https://www.psdgraphics.com/wp-content/uploads/2015/04/fingerprint.jpg>.
- [7] *Atlassian, Jira* [online]. [cit. 25.01.2020]. Dostupné z: <https://www.atlassian.com/cs/software/jira>.
- [8] *BambooHR* [online]. [cit. 25.01.2020]. Dostupné z: <https://www.bamboohr.com>.
- [9] *OrangeHRM* [online]. [cit. 25.01.2020]. Dostupné z: <https://www.orangehrm.com>.
- [10] *Toggl* [online]. [cit. 25.01.2020]. Dostupné z: <https://toggl.com>.
- [11] *Zákon č. 262/2006 Sb., zákoník práce*.
- [12] *RFID Radio Frequency and Identification: Applications and Implications Consumers*. Březen 2005. Dostupné z: <https://www.ftc.gov/sites/default/files/documents/reports/rfid-radio-frequency-identification-applications-and-implications-consumers-workshop-report-staff/050308rfidrpt.pdf>.
- [13] *The Use of RFID for Human Identity Verification*. Prosinec 2006. Report No. 2006-02. Dostupné z: https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf.
- [14] AHN, L. von, BLUM, M. a LANGFORD, J. *TELLING HUMANS AND COMPUTERS APART AUTOMATICALLY* [online]. February 2004 [cit. 15.02.2020]. Dostupné z: http://www.cs.cmu.edu/afs/cs/Web/People/aladdin/papers/pdfs/y2004/captcha_cacm.pdf.

- [15] DAS, R. *Biometric technology : authentication, biocryptography, and cloud-based architecture*. ISBN 978-1-4665-9245-2.
- [16] EMPEY, C. *How to create a strong password* [online]. August 2018 [cit. 24.2.2020]. Dostupné z: <https://blog.avast.com/strong-password-ideas>.
- [17] HAMERNÍK, B. J. *Autentizační metody používané k obnově přihlašovacího hesla*. Jaro 2014 [cit. 16.02.2020]. Dostupné z: https://is.muni.cz/th/j42vm/diplomova_prace.pdf.
- [18] JELÍNEK, M. *Daktyloskopie - historie, současnost a budoucnost*. Říjen 2014 [cit. 17.02.2020]. Dostupné z: <https://is.cuni.cz/webapps/zzp/detail/129572/>.
- [19] MEMON, S., SEPASIAN, M. a BALACHANDRAN, W. Review of finger print sensing technologies. In: Leden 2009, s. 226 – 231.
- [20] MERTLÍK, T. *Technologie NFC a její zabezpečení*. Květen 2013. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2013. 116 s.
- [21] MGR. ING. RADOMÍR ŠČUREK, P. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. Červen 2008 [cit. 15.02.2020]. Dostupné z: http://alfanomy.com/PDF/biometricke_metody.pdf.
- [22] SECURITY, D. *Salted Password Hashing - Doing it Right* [online]. June 2019 [cit. 25.2.2020]. Dostupné z: <https://crackstation.net/hashing-security.htm>.
- [23] SQUARE, I. [online]. Prosinec 2015 [cit. 18.02.2020]. Dostupné z: <http://nearfieldcommunication.org>.
- [24] WANT, R. An Introduction to RFID Technology. *IEEE Pervasive Computing*. Los Alamitos, CA, USA: IEEE Computer Society. Leden 2006, roč. 5, č. 01, s. 25–33. ISSN 1558-2590.
- [25] ŠETELÍKOVÁ, A. *Pojem a podstata daktyloskopie*. Listopad 2012. Univerzita Karlova v Praze, Právnická fakulta.

Příloha A

Obsah CD

```
xbarto92
├── bp.pdf
├── latex
├── readme
├── src
│   ├── app
│   │   ├── app.js
│   │   ├── cert.pem
│   │   ├── Dockerfile
│   │   ├── downloads
│   │   ├── js
│   │   ├── key.pem
│   │   ├── package.json
│   │   ├── package-lock.json
│   │   ├── public
│   │   ├── views
│   │   └── wait-for-it.sh
│   ├── database
│   │   ├── init.sql
│   │   └── root.sql
│   ├── docker-compose.yml
│   └── Makefile
```