**ТЕХНОЛОГИЧНО УЧИЛИЩЕ ЕЛЕКТРОННИ СИСТЕМИ**

**към ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**

**ДИПЛОМНА РАБОТА**

Тема: IoT система за отдалечен достъп, контрол и анализ на устройства

|  |  |
| --- | --- |
| Дипломант: | Научен ръководител: |
| *Огнян Барух* | *Атанас Атанасов* |

СОФИЯ

2 0 2 1

УВОД

През последните години терминът “IoT” (Internet of Things – Интернет на нещата) придобива огромна популярност, тъй като такива решения улесняват нашето ежедневие. Вече съществуват решения, които ни позволяват по-лесно да контролираме нашите домове, коли, градини и други. Интернет на нещата навлиза и в проекти, свързани със сигурността, измерването и предаването на данни, както и с идентификация на лице, глас и пръстов отпечатък.

Машинното самообучение също става основен фактор в множество софтуерни и хардуерни решения през последните години. Развитието на машините позволява да бъдат тренирани по-сложни алгоритми с цел постигане на по-точни резултати. Машинното самообучение навлиза в света на технологиите все повече и повече, което ни позволява да заменим човешките усилия с работа на машини. То е използвано както за лични проекти, така и за глобални решения с цел подобряване на услуги като градски транспорт, имейл, персонални асистенти, преводи и други.

Целта на настоящата дипломна работа е да бъде изградена система, която комбинира две от най-широко използваните технологии и която създава по-лесен и по-сигурен начин за влизане в нашия дом, както и начин да следим кой е влязъл или се опитва да влезне в нашия дом. Основните компоненти на дипломната работа са камера, която засича обекти, и алгоритъм за машинно самообучение, който проверява дали засечените обекти са хора и дали тези хора са в списъкa с позволени хора, за да отключи вратата и да ги пусне в техния дом.

**ГЛАВА I. МЕТОДИ И ТЕХНОЛОГИИ НА РЕАЛИЗАЦИЯ. ПРОУЧВАТЕЛНА ЧАСТ**

**1.1 Лицево засичане**

**1.1.1 Определение**

Лицевото засичане е технология, използвана в множество решения за идентифициране на човешки лица в изображения или във видео връзки на живо. То произлиза от засичането на обекти, като в случая търсените обекти са човешки лица. Един алгоритъм за лицево засичане се тренира върху множество изображения на различни човешки лица – различни полове, различни раси, различни черти на лицето. При изпълняване на алгоритъма той обхожда пиксел по пиксел даденото изображение и сравнява пикселите със съществуващите снимки на лица, за да открие приликите между тях. В зависимост от приликите между потенциалното засечено лице и снимките на познатите лица, алгоритъмът „взима решение“ дали даденият обект е лице или не, като резултатът е процентът сигурност, че разглежданият обект е лице. Съществуват алгоритми, които се тренират по време на изпълнение – при засечено лице алгоритъмът го добавя към множеството от познати лица. По този начин всяко следващо разпознато лице довежда до по-точни резултати.

**1.1.2 Приложения**

Лицевото засичане намира множество приложения в различни сфери –системи за лицево разпознаване, автоматичен фокус във фотографията, разпознаване на емоции, както и четене по устни. С развиването на алгоритмите и моделите за лицево засичане, то набира все повече и повече популярност в различни решения.

**1.2 Лицево верифициране**

**1.2.1 Определение**

Лицевото верифициране използва резултатите от лицевото засичане, за да сравни непознато лице с познати такива. За разлика от лицевото разпознаване, което отговаря на въпроса: „Чие е това лице?“, лицевото верифициране отговаря на въпроса: „Това ли е правилното лице?“. Един алгоритъм за лицево верифициране сравнява характерните черти на непознатото и познатите лица – разстоянието между зениците на двете очи, разстоянието между външния и вътрешния ъгъл на всяко око, разстоянието между носа и устата и други. Тази информация се записва като вектор със 128 измерения, а впоследствие се сравняват данните от всички измерения, за да се верифицира непознатото лице.

**1.2.2 Приложения**

Лицевото верифициране намира широко приложение в системи, свързани със сигурността, като това могат да бъдат както лични системи, така и публични такива. Лицевото верифициране се използва за контрол на достъпа до различни помещения, както и за отключване на нашите смартфони.

**1.3 MQTT**

**1.3.1 Определение**

MQTT представлява стандартен протокол за комуникация, който намира широко приложение в проектите, свързани с „Интернет на нещата“.

**1.3.2 Принцип на работа**

MQTT работи на принципа на публикуване и абониране за съобщения, което позволява едно съобщение да достига до множество крайни устройства. Всяко устройство може да се абонира за даден канал и да получава всички съобщения в този канал.

**1.3.3 Защо MQTT е толкова разпространен?**

Най-силните страни на MQTT, е че има много висока скорост и много ниска комуникация. Една MQTT заявка се изпълнява над 10 пъти по-бързо от една HTTP заявка. Освен това този протокол е с малко, но все пак достатъчни възможности, за да се постигнат необходимите функционалности за работа с устройства. MQTT заявките са с много малък размер, което позволява на устройства с ограничени възможности да се възползват от услугите на този протокол. MQTT позволява една съобщение да бъде получено от безброй много абонати, докато при HTTP ще трябва да се изпращат отделни съобщения до всеки получател.

**1.4 Дигитални близнаци**

Дигитален близнак на едно устройство представлява съвкупността от информация, описваща съществуващо устройство. Терминът добива популярност в началото на XIX век с навлизането в ерата на „Интернет на нещата“. Дигиталният близнак може да се разглежда като база от данни за едно устройства, съдържаща само текущата информация. Ако устройството има връзка със своя дигитален близнак, то тогава то може да сигнализира за промяна в неговата информация, която да се отбележи в дигиталния близнак. Съществуването на дигитални репрезентации позволява на хората да следят от разстояние информацията и работата на всяко устройство.

**1.5 Bosch IoT Suite**

**1.5.1 Определение**

Bosch IoT Suite представлява платформа за свързване на устройства, тяхното контролиране, както и обработването на данните, които изкарва всяко устройство. Услугите в Bosch IoT Suite са разделени спрямо функционалността си – свързване на устройства, дигитална репрезентация на устройства, управление на устройства и подновяване на софтуера върху устройства. Към днешна дата над 15 милиона устройства са свързани към Bosch IoT Suite. Също така над 250 международни проекта се възползват от услугите, предлагани от тази платформа.

**1.5.2 Bosch IoT Hub**

Bosch IoT Hub представлява облачна услуга, която свързва устройства с приложения, които ги управляват. Чрез тази услуга разработчиците на софтуер получават бърз и лесен начин да свържат най-различни устройства към своите приложения. Тя поддържа няколко протокола за комуникация, най-известните от които са HTTP, MQTT и AMQP. Свързването на устройства чрез Bosch IoT Hub е лесно и най-вече сигурно, тъй като се разчита на информация, достъпна само за притежателя на устройствата.

**1.5.3 Bosch IoT Edge Services**

Bosch IoT Edge Services представлява връзката между устройствата и тяхната дигитална репрезентация в Bosch IoT Suite. Освен връзката, Bosch IoT Edge Services осъществява и комуникацията между едно устройство и Bosch IoT Suite посредством протокола MQTT. Те позволяват на устройства, работещи върху всякакви протоколи, да се свържат със своя дигитален близнак. По този начин всяко устройство, което работи с Bluetooth, Z-Wave, ONVIF, ZigBee и други може по много бърз и лесен начин да се свърже и управлява чрез Bosch IoT Suite.

**1.6 Ключалка**

За отключване на вратата съм избрал ключалка Danalock V3 Smartlock. Тази ключалка може да бъде свързана към смартфон или към смарт часовник и да се контролира от съответното устройство. Ключалката използва протокола Z-Wave за комуникация. Този протокол позволява лесното ѝ свързване към Bosch IoT Suite, както и лесното задаване на команди към нея. Освен това тя може да бъде контролирана през Wi-Fi, а създателите на тази ключалка са разработили и мобилно приложение, което може да се свърже с нея и да я контролира.

**1.6.1 Z-Wave**

Z-Wave представлява протокол за безжична комуникация, като се използва предимно в решения, свързани с „Интернет на нещата“. Най-често протоколът се използва, за да се осъществи комуникацията с устройства в дома като автоматични ключалки, автоматични прозорци, автоматични врати за гаражи, термостати и други. Вълните достигат до 100 метра, което позволява пълен контрол в дома и градината. Всяко устройство, поддържащо Z-Wave, може да бъде контролирано през Wi-Fi, което улеснява работата с тези устройства.

**1.7 Камера**

**1.7.1 ONVIF**

ONVIF е глобална организация, която цели да стандартизира работата с базираните на IP устройства, свързани със сигурността. Създаденият стандарт описва връзката и комуникацията между различни устройства за видеонаблюдение и централни машини, които следят тяхната работа и потока, който записват. Друга основна цел на организацията е да се осигури съвместимостта между продукти на различни компании, за да се постигне по-сигурна и стандартна система.

**ГЛАВА II. ИЗИСКВАНИЯ КЪМ ПРИЛОЖЕНИЕТО. ПРОГРАМНА РЕАЛИЗАЦИЯ**

**2.1 Изисквания към приложението**

**2.1.1 Изисквания към модела за лицево верифициране**

• Моделът за лицево верифициране да включва програма, която да позволи на потребителя да отвори камерата на машината си и да снима изображения на потребителя, с които да се тренира алгоритъма.

• Моделът за лицево верифициране да включва модел за лицево засичане, който да засича всички лица на хора в едно изображение и да ги запазва в масив.

• Процесът за лицево верифициране да прекъсва изпълнението си, ако няма засечени лица в изображението.

• Моделът за лицево верифициране да включва програма, която да тренира алгоритъма, използвайки заснетите снимки за познати лица.

• Моделът за лицево верифициране да включва програма, която да приема изображение чрез хипервръзка или чрез файл с възможни разширения .jpg, .png и .jpeg. Програмата трябва да засече всички лица в изображението и да провери кои лица са на познати хора. Алгоритъмът трябва да връща масив с познатите засечени лица или „Unknown”, ако сред засечените лица няма нито едно познато.

**2.1.2 Изисквания към системата от свързани устройства**

• Системата да включва Raspberry Pi, което да има инсталирани Bosch IoT Edge Services, за да може да се свържат устройствата в система към това Raspberry Pi.

• Системата да включва камера, която да е свързана към Raspberry Pi посредством Bosch IoT Edge Services. Тази камера трябва да засича движение, да прави снимка и да изпраща хипервръзка на снимката към Raspberry Pi, за да се верифицират човешките лица, ако има такива.

• Системата да включва ключалка, която да е свързана към Raspberry Pi посредтсвом Bosch IoT Edge Services. Ключалката да се отключва за 5 секунди, ако моделът за лицево верифициране разпознае лице. Съобщенията към ключалката да се изпращат и получават посредством Z-Wave контролер, свързан към Raspberry Pi.

**2.1.3. Изисквания към мобилното приложение**

• Мобилното приложение да може да изпраща HTTP заявки към Bosch IoT Suite с цел достъп, четене и редактиране на дигиталните близнаци на устройствата.