Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.738.5:339
DOI: https://doi.org/10.24867/28BE14Vulin

СИСТЕМ ЗА ПРАЋЕЊЕ ПРИСУСТВА НА ДОГАЂАЈИМА

SYSTEM FOR MONITORING PARTICIPATION IN EVENTS

Светозар Вулин, *Факултет техничких наука, Нови Сад*

Област - РАЧУНАРСТВО И АУТОМАТИКА

Кратак садржај – *У овом раду је описано решавање проблема праћења присуства на догађајима. Рад се заснива на опису различитих проблема и представљања могућих решења. Од описаних решења, одабрано је једно решење, које је имплементирано и описано у систему АирСофт платформе.*

Кључне речи: *догађај, валидација идентитета, валидација присуства, платформа*

Abstract – *This paper describes the solution to the problem of tracking attendance at events. The work is based on the description of various problems and the presentation of possible solutions. Of the described solutions, one was selected, implemented, and described in the specific AirSoft platform system..*

Keywords: *event, identity validation, presence validation, platform*

1. УВОД

Овај рад се бави детаљним анализирањем и поређењем различитих приступа и решења за доказивање присуства особа на разним догађајима, било да су они формални или неформални, као што су спортска такмичења, конференције, предавања или приватна окупљања. Рад се бави проблемом потврде идентитета посетилаца, разматрајући како ефикасно извршити валидацију без стварања гужви, посебно на догађајима са великим бројем људи. За такве догађаје предлаже се употреба аутоматизованих система који раде без људског фактора. С друге стране, за мање догађаје са вишим захтевима за сигурношћу, потребна је детаљнија провера идентитета како би се спречила злоупотреба и крађа идентитета.

Циљ рада јесте да представи и упореди различите методе које особе могу користити да докажу своје физичко присуство на догађају, укључујући имплементацију и тестирање одабраног решења у оквиру АирСофт (АСФ) платформе. Такође, у раду су донети закључци о ефикасности имплементираног решења, потенцијална унапређења и будући развој различитих метода потврде присуства.

2. ПРОБЛЕМ ПОТВРДЕ ПРИСУСТВА НА ДОГАЂАЈИМА

Проблем потврде присуства на догађајима је чест изазов, како за веће, тако и за мање скупове. Потребно је да се провери да ли су посетиоци који долазе на догађај, заправо они који су позвани или пријављени. За веће догађаје, обично се ангажују волонтери или запослени који би вршили проверу идентитета посетилаца на улазу. То може бити временски захтевно и стресно, а такође и стварати редове и кашњења. Постоји и ризик од злоупотребе позивница и крађе идентитета. Као решење предлаже се развој система или софтвера који би убрзао и олакшао процес верификације. У раду се анализира проблем из две перспективе: корисника и администратора догађаја.

Администратор може бити организатор догађаја или неко ко има ауторитет за потврду присуства. Конкретан пример решења овог проблема анализира се у контексту АСФ платформе, која је имплементирана за организацију догађаја и валидацију присуства учесника.

2.1. Перспектива администратора

Администратор представља врсту ауторитета, односно ентитет који је одговоран за догађај, као и то да његово одржавање протекне како је планирано. Администратор треба да врши креирање догађаја, као и дефинисање времена и места одржавања. Уколико систем утврди да нису сви пријављени корисници присутни, администратор може да реагује на време. Такође, одговорност администратора је да се спречи злоупотреба позивница, лажирање идентитета, и сл. Особа која је администратор може, а не мора представљати особу која врши верификацију и може, а не мора да управља догађајем. У раду је потребно осврнути се на могуће приступе који би искључили администратора из процеса потврде делегирањем посла на систем.

2.2. Корисничка перспектива

Када се корисник пријави на догађај, очекује се да ће он бити одржан на одређеном месту и у дефинисаном времену. Важан део учешћа на догађају јесте верификација присуства корисника, која обухвата потврду идентитета и физичког присуства. Идентификација је важна због ризика од злоупотребе, као што је појављивање других особа уместо позваних, што може нарушити интегритет и приватност догађаја и створити конфликте при валидацији пријава.

Постоји проблем приватности, који се јавља приликом обраде личних података, јер могу постојати ризици од њихове злоупотребе, укључујући крађу идентитета или новчаних средстава. Због тога је тешко стећи поверење корисника и прикупљати њихове податке.

НАПОМЕНА:
Овај рад проистекао је из мастер рада чији ментор је био др Горан Сладић, ред. проф.

2.3. Кораци у решавању проблема

2.3.1. Потврда идентитета

Да би се верификовао идентитет пријављеног корисника на догађају, неопходно је проверити његов идентитет, а узимајући у обзир учесталост крађа идентитета на интернету, важно је осигурати сигурно складиштење личних података. Постоје различити методи за потврду идентитета: скенирање личног документа, поређење фотографије особе са онима у систему користећи вештачку интелигенцију и употреба јединственог идентификационог броја додељеног кориснику на платформи. Свака од ових метода има своје предности и мане, као што је ризик од крађе личног документа приликом скенирања, коришћење фотографија лошијег квалитета приликом поређења вештачком интелигенцијом, крађа јединственог броја. Алтернатива употреби јединственог броја би могао бити QR код [1], који нуди већу сигурност, и не може бити украден као број јер се не може запамтити. Ове методе захтевају баланс између сигурности и практичности у циљу ефикасне и поуздане верификације идентитета на догађајима.

2.3.2. Валидација пријаве

Након идентификације корисника, потребно је проверити да ли је његова пријава за догађај валидна и да ли се налази на списку пријављених корисника на платформи. Пријава се сматра валидном ако је корисник или добио позив од организатора догађаја или се сам пријавио путем платформе. Овај процес валидације пријаве је важан да би се осигурало да на догађају буду само они који су заиста пријављени или позвани. Валидација се врши у оквиру платформе, где се подаци из корисничког профила упоређују са списком пријављених корисника. Успешна валидација потврђује да је корисник пријављен за догађај, а након тога следи провера његовог физичког присуства.

2.3.3. Потврда физичког присуства на догађају

2.3.3.1. Потврда без присуства администратора

Уколико је потребно ослободити администратора одговорности за потврду физичког присуства, систем треба да подржи методе које се ослањају на међусобну верификацију присутних особа на догађају или да омогући корисницима да самостално потврде своје присуство. Ово подразумева дефинисање броја и начина верификација потребних за валидацију од стране других особа или развој механизма који корисницима омогућава да индивидуално верификују своје присуство скенирањем докумената или потврдом локације преко платформе.

2.3.3.2. Потврда са присуством администратора

Овај приступ се ослања на особу која представља ентитет администратора, односно особу која има већу одговорност и задужења од обичног корисника, и која би вршила улогу валидатора. Администратор има могућност да изврши потврду присуства за сваку особу која се појавила на догађају, скенирањем кода, личног документа, или неким другим видом валидације. Проблем приликом имплементације оваквог приступа је у томе што се систем ослања на администратора, што укључује фактор људске грешке и обавезе да мора да постоји особа која ће бити ауторитет и обављати посао валидације, што може резултовати временски захтевном процесу.

3. ПОРЕЂЕЊЕ РАЗЛИЧИТИХ ПРИСТУПА ПОТВРДЕ ПРИСУСТВА

3.1. Геолокацијска претрага

Геолокацијска претрага користи ГПС (енг. *Global Positioning System, GPS,* [2,3]) технологију за одређивање географске локације уређаја, као што су мобилни телефони или рачунари. Овај вид претраге се ослања на ГПС технологију, која представља мрежу сателита и пријемних уређаја, који емитују сигнал, са циљем одређивања локације уређаја на земљи. Приликом креирања догађаја, дефинише се његова локација, а корисници који су се пријавили могу да потврде своје присуство тек када физички стигну на задату локацију. Систем проверава да ли се географске координате корисника поклапају са координатама места одржавања догађаја. Могући проблем настаје ако неко други користи уређај пријављеног корисника, што се може решити додатном верификацијом идентитета, као што је скенирање личних докумената или QR кодова. Овај систем омогућава самосталну потврду присуства од стране корисника, независно од администратора.

3.2. Скенирање QR кода од стране других посетилаца

Скенирање QR кода од стране других посетилаца на догађају представља метод валидације присуства који се ослања на друге посетиоце са циљем да они изврше валидацију присуства. Корисници добијају QR код при пријави на догађај, који је валидан само за тај догађај. На догађају, корисници морају скенирати кодове других корисника и на тај начин валидирати њихово присуство. Број потребних скенирања зависи од величине догађаја и може се дефинисати од стране администратора. За мање догађаје, потребно је да свака особа скенира свачији QR код, док за веће догађаје може постојати одређена граница скенирања. Овај метод повећава ниво заштите, јер га је теже заобићи са повећањем броја потребних скенирања. На примеру АСФ платформе, администратор може поставити лимит да је потребно скенирање од најмање 60% присутних, што осигурава чињеницу да и играчи из супротних тимова морају међусобно скенирати кодове. Ово омогућава да се валидација обави без укључивања администратора, али може бити временски захтевно и потенцијално лоше за корисничко искуство.

3.3. Скенирање QR кода од стране ауторитета

Скенирање QR кода од стране ауторитета је метод валидације где особа са ауторитетом скенира QR код генерисан од стране система након пријаве корисника на догађај. Овај код је специфичан за сваки догађај и не може се злоупотребити за друге догађаје. Овај приступ обједињује валидацију идентитета и потврду присуства, а валидацију пријаве врши систем.

Предности укључују једноставност употребе и решавање оба проблема од стране једне особе без потребе за додатним системима. Међутим, овај метод може бити временски захтеван и напоран за особу која се сматра ауторитетом, посебно на већим догађајима, што може довести до негативног корисничког искуства због дугог чекања на валидацију.

3.4. Коришћење NFC технологије за скенирање

NFC (енг. *Near Field Communication*) [4,5] технологија омогућава комуникацију између уређаја на кратким раздаљинама (до 4 цм), ослањајући се на радио комуникацију. Често се користи у паметним уређајима [6] за разне сврхе као што је бежично плаћање. *NFC* може заменити традиционалне методе валидације присуства као што су скенирање QR кодова. Уместо QR кодова, корисници могу користити *NFC* за међусобну верификацију присуства или за верификацију од стране ауторитета. Ова технологија олакшава процес скенирања, смањујући време потребно за валидацију и побољшава корисничко искуство. *NFC* може бити коришћен и за скенирање личних докумената као што су биометријски пасоши. Предности *NFC*-а укључују бржу валидацију и боље корисничко искуство, док је мана што можда немају сви корисници уређаје компатибилне са *NFC* технологијом.

4. СПЕЦИФИКАЦИЈА СИСТЕМА

4.1. Спецификација апликације и изазови

АСФ је спорт заснован на симулацији рата, где се користе реплике оружја и различити приступи игри, који се могу организовати на различитим теренима, у зависности од броја играча. Циљеви игре укључују елиминисање противничког тима, постављање бомби или освајање заставица.

АСФ платформа је мобилна апликација која омогућава креирање и организацију догађаја, турнира и тимова. Главни изазови у имплементацији решења за валидацију присуства корисника укључују питања сигурности, као што су заштита корисничких података, интегритет платформе и робусност самог решења. За обезбеђивање сигурности система важни су механизми као што су контрола приступа [7], ауторизација и аутентификација [8], као и складиштење хешованих (енг. *hash,* [9]) података у бази података. Интегритет система се односи на његово поуздано функционисање, док робусност решења подразумева да сви корисници који присуствују догађају буду успешно и поуздано валидирани.

4.2. Спецификација система

Систем се састоји од три главне компоненте: сервера, скенера и корисничке апликације. Сервер представља логичку компоненту, која је задужена за складиштење података и служи да би се прибавили подаци који су потребни за валидацију у одређеном тренутку. Скенер представља уређај који је повезан на платформу, и даје јој одобрење да користи његову камеру. Између сервера и скенера се дешава константна комуникација, из разлога што скенер све податке које прочита и валидира, шаље серверу, који даље врши валидацију и потврду да ли је процес извршен успешно или није. Корисничку апликацију користе корисници да би комуницирали са платформом, како би се пријавили на догађај и потврдили своје присуство на истом. Они у корисничкој апликацији имају преглед свих догађаја који су креирани, и имају могућност да се пријаве на жељени догађај. Када се корисник пријави, и дође време за одржавање догађаја, корисник мора да валидира своје присуство користећи опције из корисничке апликације. Скенер прво скенира QR код који корисник приложи из апликације, и затим се обавља провера идентитета. Након тога корисник може да обави верификацију да се налази на догађају помоћу геолокацијске претраге.

5. ИМПЛЕМЕНТАЦИЈА СИСТЕМА

5.1. Архитектура система

Као што је већ наведено у одељку 4.2., систем се састоји из три главне компоненте. За изградњу изгледа и корисничког интерфејса, као и интерфејса који користи скенер, коришћена је библиотека *React.js*. За имплементацију скенер компоненте и система за читање и дешифровање QR кодова, коришћена је нпм (енг. *npm*) библиотека *react-qr-reader*. За сервер је коришћен *Node.js* и око њега радни оквир (енг. *framework*) *genzy.io* који се ослања на *Express.js* радни оквир. За чување података је коришћена *NoSQL* база података *MongoDB.*

5.2. Потврда валидације идентитета скенирањем QR кода

Приликом регистрације на платформу, сваки корисник након што је унео своје податке, добија јединствени QR код, који касније може да искористи у сврху валидације. Овај код не би требао да се дели са другима, да не би био злоупотребљен. Он једнозначно одређује власника профила и садржи његове личне податке.

Приликом скенирања, потребно је да корисник принесе свој уређај (на којем се налази QR код) скенеру, који затим врши скенирање и валидацију података. Након што су прочитани подаци са QR кода, потребно их је упоредити са подацима тренутно улогованог корисника. Валидација се обавља тако што се подаци који су сачувани приликом пријављивања на догађај, пореде са подацима који се налазе складиштени у QR коду. Уколико се информације поклапају, корисник је валидиран и његово присуство је успешно потврђено од стране система.

5.3. Имплементација геолокацијске претраге

Као што је објашњено у одељку 3.1., геолокацијска претрага представља претрагу по географској ширини и дужини. Након што је корисник дошао на догађај, потребно је да валидира своје присуство, тако што ће упоредити своју локацију, са предвиђеном локацијом за догађај. Ова радња се изводи тако што корисник у апликацији треба да означи да жели да потврди своје присуство коришћењем свог географског положаја (Листинг 1.). Предуслов за ову операцију јесте да је корисник одобрио апликацији да користи локацију његовог уређаја.

Након послатог захтева за валидацију, уређај преузима тренутну локацију и шаље је платформи.

```
navigator.geolocation.getCurrentPosition(
(position) => {
   const latitude =
position.coords.latitude;
   const longitude =
position.coords.longitude;

   callback({ latitude, longitude },
eventPosition, thresholdInMeters);
 });
```

Листинг 1. *Прибављање географских координата*

Након што је платформа преузела тренутну локацију, врши се претрага у бази података и проналази се локација која је дефинисана за предвиђени догађај. Из разлога што је геолокација прецизна до неколико метара, потребно је задати одређени праг толеранције, који ће се користити у рачунању могућег опсега у ком треба да се налази уређај да би његова локација била иста као и за дефинисани догађај. Рачунање дистанце између локације корисника и локације задате приликом креирања догађаја рачуна се помоћу помоћне библиотеке *geolib* [10].

```
export const checkIsSamePosition =
(userPosition, eventPosition, threshold)
=> {
 return geolib.getDistance(userPosition,
eventPosition) < threshold;
}
```

Листинг 2. *Функција за поређење локација са толеранцијом*

Успешном потврдом да је корисник стварно на задатој локацији, његов захтев бива прихваћен.

6. ЗАКЉУЧАК

У овом раду описан је проблем који се тиче доказивања присуства особе на догађају. Како догађај представља било који вид окупљања, формални или неформални, потребно је било навести различите приступе, као и њихове концепте који се користе у решавању овог проблема. У зависности од тога који се догађаји креирају, могуће је изабрати различите приступе и решења. Након поређења решења, одабрана је и описана идеја решења на примеру АСФ платформе. Након тога је дат кратак опис платформе и проблема који се јавља у конкретном случају. Одабрани начини за решавање проблема стављени су у конкретан контекст платформе, описани су изазови који су се јављали приликом имплементације, и приказано је решење у конкретном систему.

Потенцијално унапређење ових решења може да се огледа у напретку саме технологије, где би АИ пружао веродостојније начине за валидацију идентитета, масовнију употребу и имплементацију *NFC* чипова у уређаје, што би омогућило усвајање *NFC* приступа потврде, као и развој нових технологија сличних *NFC*, које би довеле до потенцијалних нових решења и приступа у решавању оваквих проблема.

7. ЛИТЕРАТУРА

[1] Tiwari, Sumit. "An introduction to QR code technology." 2016 international conference on information technology (ICIT). IEEE, 2016.

[2] Gentile, Camillo, et al. Geolocation techniques: principles and applications. Springer Science & Business Media, 2012.

[3] El-Rabbany, Ahmed. Introduction to GPS: the global positioning system. Artech house, 2002.

[4] Du, Hongwei. "NFC technology: Today and tomorrow." International Journal of Future Computer and Communication 2.4 (2013): 351.

[5] Al-Ofeishat, Hussein Ahmad, and Mohammad AA Al Rababah. "Near field communication (NFC)." International Journal of Computer Science and Network Security (IJCSNS) 12.2 (2012): 93.

[6] Silverio-Fernández, Manuel, Suresh Renukappa, and Subashini Suresh. "What is a smart device?-a conceptualisation within the paradigm of the internet of things." Visualization in Engineering 6.1 (2018): 1-10.

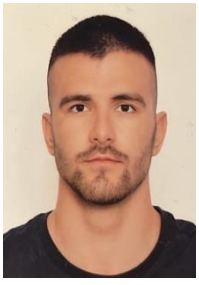
[7] Sandhu, Ravi S., and Pierangela Samarati. "Access control: principle and practice." IEEE communications magazine 32.9 (1994): 40-48.

[8] Kim, Hokeun, and Edward A. Lee. "Authentication and Authorization for the Internet of Things." IT Professional 19.5 (2017): 27-33.

[9] Sobti, Rajeev, and Ganesan Geetha. "Cryptographic hash functions: a review." International Journal of Computer Science Issues (IJCSI) 9.2 (2012): 461.

[10] https://www.npmjs.com/package/geolib

Кратка биографија:



Светозар Вулин рођен је у Руми 1999. год. Основне академске студије је завршио 2022. године на Факултету техничких наука у Новом Саду. Мастер рад на Факултету техничких наука из области Рачунарство и аутоматика – Електронско пословање одбранио је 2024. године.