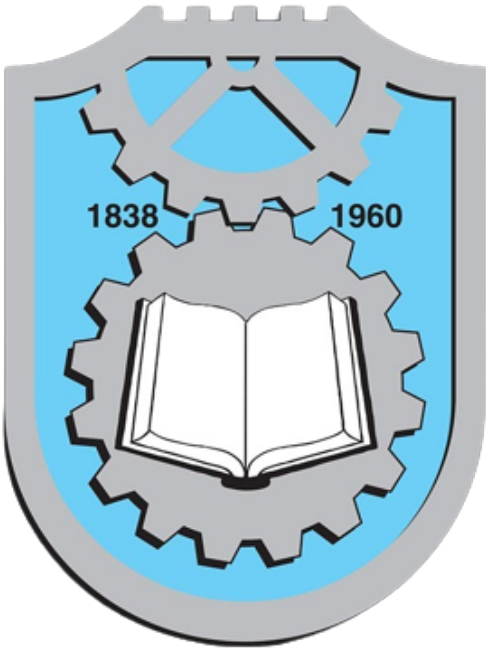
Универзитет у Крагујевцу
Факултет инжењерских наука



Развој апликација интернета ствари

Семестрални рад

Принципи, технике и примене *Machine Learning* технологија у оквиру *IoT* система

Професор:
Проф. др Милан Чабаркапа

Студент:
Каришић Ђорђе 393/2023

__.__.2023.

Садржај

1 Увод

У данашњем друштву, Интернет ствари (*Internet of Things* – скраћено '*IoT*') представља значајан аспект технолошког напретка, утичући на начин на који уређаји и системи комуницирају, сарађују и заједно обављају задатке. Способност предмета да комуницирају и размењују податке у реалном времену отвара могућности за развој различитих апликација и сервиса. Овакав развој технологија захтева иновативан приступ у управљању и обради података у реалном времену. У том контексту, технологије машинског учења (*Machine Learning*) представљају неизоставан елемент за обраду и анализу обимних и сложених података у реалном времену који произлазе из сензора (потенцијално и других елемената) *IoT* уређаја [1].

Овај семестрални рад истражује принципе, технике и примене *Machine Learning* технологија у оквиру *IoT* система. Посебан фокус стављен је на анализу како машинско учење може значајно унапредити функционалности и ефикасност *IoT* уређаја и апликација. Рад обухвата различите аспекте, укључујући методе обраде података, алгоритме машинског учења и њихову интеграцију у *IoT* архитектуру.

Истраживање вођено у оквиру овог рада има за циљ да представи анализу везе између машинског учења и *IoT* технологија, и да истакне како ова синергија може допринети напретку у различитим областима, укључујући паметне градове, здравство, заштитне системе, и индустријске системе.

Кроз примере и проучавање различитих случајева имплементације датих уско везаних технологија, рад ће илустровати конкретне врлине које примена машинског учења може донети у контексту развоја Интернета ствари. Фокус ће бити на истраживању више различитих техника машинског учења, са конкретним примером примене метода дубоког учења. Применом тих техника, може се проучити како *IoT* системи могу ефикасније обрађивати и анализирати велике количине података који произилазе из различитих сензора и уређаја.

У наставку рада, различите методологије и апликације ће бити детаљно размотрене, са фокусом на изазовима и могућностима које произилазе из интеграције ових два напредна концепта. На крају, биће изложени закључци и предложени правци за будућа истраживања у овој области.

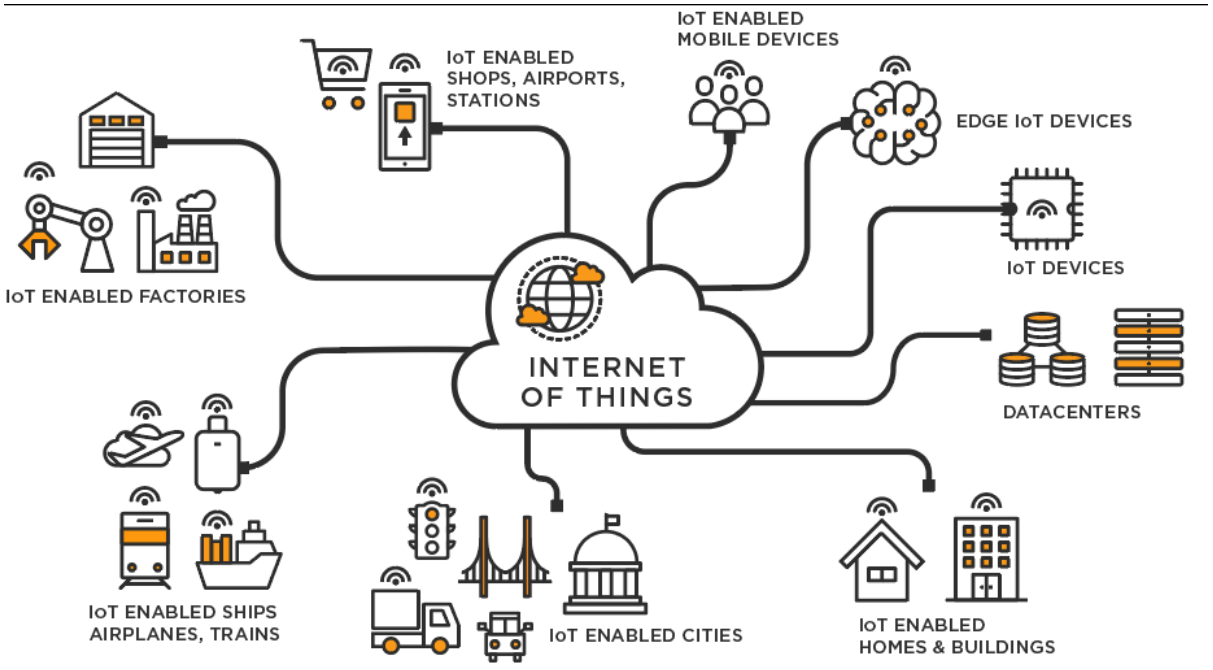
2 Интернет ствари (IoT)

Интернет ствари (IoT) представља концепт који обухвата повезивање физичких уређаја и објеката на интернету, омогућавајући им да размењују податке и информације. Ово савремено технолошко подручје обухвата широк спектар уређаја, укључујући сензоре, актуаторе, уграђене системе, и све више свакодневних објеката који постају 'паметни'.

Сензори уграђени у различите уређаје могу пратити услове у околини, примати информације о стању уређаја, и комуницирати преко мреже. Различите области се користе IoT решењима. У сфери здравства, IoT сензори прате виталне информације пацијената и дају излазне податке о лечењу. У индустрији, паметни сензори и актуатори обезбеђују аутоматизацију и побољшавање управљања ресурсима. У сфери транспорта, IoT омогућава паметно управљање саобраћајем и праћење транспортних средстава.

Основна карактеристика IoT-а је способност прикупљања и размене података, често у реалном времену. Уређаји и објекти који нису традиционално имали могућност комуникације сада постају паметни и контролишу се путем мрежа. Ово је јако иновативно решење, које отвараја нове начине за паметно и ефикасно коришћење ресурса, смањење трошкова и подизање квалитета живота.

Сликом 1 дат је илустративни пример разноликих индустрија и области у којима IoT системи налазе примену.



Слика 1: Разноликост области у којима се примењују IoT системи [2]

IoT са собом носи идеје о иновацијама у областима као што су вештачка интелигенција и машинско учење. Способност да се анализирају и користе огромне количине података које генерише IoT систем отвара пут за врло ефикасно обучавање модела машинског учења и тиме прецизно предвиђање резултата.

3 Предности употребе метода машинског учења у *IoT* системима

Употреба машинског учења у системима Интернета ствари (IoT) доноси многе предности које значајно утичу на функционалности и ефикасност ових система [3]. Неке од кључних предности укључују:

П.1 Ефикасна обрада података
Методе машинског учења омогућавају системима Интернета ствари брзу, ефикасну и поуздану обраду великих количина података различитих формата, прикупљених од стране сензора и других уређаја који се налазе у оквиру IoT система. Ове методе могу идентификовати обрасце и шаблоне који се могу пронаћи у оквиру података и извући информације од значаја из њих. Овиме се постиже моделирање система који прецизно пресликава и везује карактеристике и вредности из података – што води до решавања задатака у реалном времену са високим степеном учинка.

П.2 Аутоматизација и Оптимизација
Машинско учење омогућава IoT системима да сами уче из искуства, потенцијално без надгледања, важност информација које им долазе на улаз и тиме оптимизују своје радне параметре (једноставније речено, могу оптимизовати хиперпараметре својих метода машинског учења) што их чини 'свесним' што се тиче података са којима раде. Појам такозване 'свести' у овом контексту дефинише динамичну природу система, тј. могућност да се прилагоди подацима. Примера ради, системи за управљање енеријом могу применити методе машинског учења како би интелигентније регулисали потребе за енергијом, на основу карактеристика и обичаја корисника везаних за потрошњу дате енергије.

П.3 Одржавање уређаја и система
Машинско учење може предвидети и потенцијално спречити неисправности уређаја у оквиру IoT система. Методе машинског учења могу анализирати податке прикупљене са сензора и предвидети могуће проблеме, што доводи до превенције тих проблема и умањивања времена уређаја у неактивном режиму – умањујући трошкове.

П.4 Прилагодљивост и скалабилност
Како је претходно наведено у П.2, методе машинског учења омогућавају IoT системима да буду прилагодљиви на промене у околини. За систем који је способан да се ефикасно прилагоди променама у околини без значајнијих губитака у учинку, без обзира на број, формат и тачност података се може рећи да је **скалабилан**. Скалабилност је јако важан фактор у IoT системима, поготово у динамичним окружењима, где број уређаја и обим података доста варира.

П.5 Безбедност и Приватност
Алгористми машинског учења могу помоћи у откривању необичних или потенцијално опасних активности у мрежи IoT система. Примена алгоритама машинског учења у борби са сигурносним опасностима у мрежама система може значајно повећати ниво безбедности мреже и заштите приватности.

4 Интеграција метода машинског учења у *IoT* системе

Машинско учење представља поље вештачке интелигенције, чије методе се примењују, уз помоћ модерног рачунарства у готово свакој индустрији и пољу науке. Разлог широке примене машинског учења је, поред свега, како је претходно наведено, прилагодљивост подацима са којима ради.

4.1 Типови података у *IoT* системима

У оквиру једног *IoT* система могу кружити разни типови података, у различитим форматима, чија обрада представља главни задатак методама машинског учења при интеграцији истих са *IoT* системима.
Како би се јасније дефинисала разноликост података у једном *IoT* систему, потребно је издвојити пар врста (формата) података који се најчешће уочавају као исход мерења сензора у таквим системима:

- **Визуелни подаци**
  У системима за надгледање безбедности у градовима, камере могу прибављати визуелне податке попут слика или видео записа са улица или других јавних простора. Такви подаци се могу користити за анализу саобраћаја, људске активности или препознавања одређених објеката.

- **Нумерички подаци**
  Нумерички подаци могу представљати температуру прочитану са термостата у згради, кући или неком јавном простору. Та нумеричка вредност која представља температуру се може користити за аутоматско регулисање система хлађења или грејања, са циљем оптимизације потрошње или одржавањем предефинисане вредности прага температуре коју је корисник поставио.

- **Категоријски подаци**
  У паметној расвети, стања извора светла (стања 'укључено' и 'искључено') могу представљати категоријске податке. Сваки извор светла мора бити у једном и само једном од тих датих стања. Такви подаци се могу користити за даљинско управљање расветом путем мобилне апликације или платформе за управљање расветом.

- **Временски осетљиви подаци**
  Сензори распоређени широм града могу сакупљати податке о тренутним временским условима. Такви подаци се могу користити за предвиђање будућих временских услова, попут влажности ваздуха, температуре или брзине ветра.

- **Аудио (звучни) подаци**
  Један *IoT* систем може бити употребљен за препознавање гласних инцидената, попут пуцњаве из ватреног оружја или експлозије, или за одржавање нивоа квалитета звука на јавним наступима и сличним догађајима.

Са претходне листе, може се приметити да постоје бројни типови података који могу циркулисати у оквиру једног *IoT* система, што говори о томе да, интеграцијом метода машинског учења, можемо знатно унапредити учинак и безбедност тог система, чинећи га 'паметнијим' и прилагодљивијим условима околине.

4.2 Машинско учење – методи, задаци и примери употребе

На машинско учење се може гледати као на скуп метода са разним приступима обради података, са различитим задацима, предностима и манама чија примена може бити самостална или у комбинацији са другим методама.
Машинско учење може се класификовати у различите категорије у складу са различитим приступима, задацима и типовима обраде података. У оквиру ове области, можемо извршити генерализацију задатака и проблема на следећи начин:

- Надгледано машинско учење (енг. *Supervised learning*)
- Ненадгледано Машинско Учење (енг. *Unsupervised learning*)
- Учење са подршком (учење уз подстицаје) (енг. *Reinforcement learning*)

4.2.1 Надгледано машинско учење

Надгледано машинско учење је приступ у коме модели уче из парова улазних и излазних података. Током обучавања, модел се прилагођава тако да може тачно предвидети излазне вредности на основу нових, непознатих улаза. Овакав приступ обично захтева велики скуп анотираних података за обучавање.
Основни задаци надгледаног машинског учења су:

1. **Класификација**
   Опис: Тип задатака где је потребно улазне податке прикружити једној или више предефинисаних категорија, на основу карактеристика улазних података.
   Пример(и): Класификација пиксела на основу интензитета зарад сегментације улазне слике, класификација мејлова на легитимне и спам мејлове, детекција објеката на слици.

2. **Регресија**
   Опис: Задатак у којем модел предвиђа континуалне и нумеричке излазне вредности на основу улазних података.
   Пример(и): Предвиђање цена некретнина на основу броја соба, површине или локације, предвиђање времена доставе производа на основу удаљености и гужве у саобраћају.

4.2.2 Ненадгледано машинско учење

Ненадгледано машинско учење је приступ где модели уче из улазних података без претходно анотираних излазних података. Овај приступ је често коришћен када је теже добити анотације за велики скуп података.
Основни задаци ненадгледаног машинског учења укључују:

1. **Кластеровање**
   Опис: Груписање сличних инстанци улазних података без унапред дефинисаних категорија.
   Пример(и): Груписање корисника у више врста на основу купљених производа у онлајн продавници, груписање филмова на основу сличности, тј. заједничких или сличних глумаца, жанрова, језика и описа, генерисање вештачких примерака података који су слични по структури и карактеристикама улазним подацима.

4.2.3 Учење са подршком

Учење са подршком представља приступ у машинском учењу где агент учи како да интерагује са околином тако да максимизује награду. Овај приступ се користи у ситуацијама где модел не поседује конкретне анотације за улазне податке и излазне акције.
Како у оквиру овог типа учења постоји само један задатак – да агент максимизује награду и научи да интерагује са средином, потребно је навести елементе који чине учење са подршком и омогућавају извршавање задатка, који укључују:

1. **Околина**
   Опис: Систем са којим агент интерагује и из којег добија информације.
   Пример: Виртуелни свет у коме се агент обучава за управљање.

2. **Награда**
   Опис: Повратна информација коју агент добија из околине након сваке извршене акције.
   Пример: Учење агента за играње видео игре где је награда освојени бод.

3. **Стање**
   Опис: Репрезентација тренутног стања у околини које се користи за одлучивање о наредној акцији.
   Пример: За агента који учи шах, стање би било тренутна распоред фигура на табли.

4. **Акција**
   Опис: Понашање или корак који агент прави у одређеном стању како би дошао до наредног.
   Пример: У шаху, акција би могла бити померање фигуре на табли.

5. **Политика (енг. *Policy*)**
   Опис: Скуп правила или стратегија које агент користи за одабир акција у одређеним стањима.
   Пример: За агента који игра видео игру, политика би била стратегија избора акција како би максимизовао награду.

Учење са подршком најчешће се користи у ситуацијама када је потребно оптимизовати секвенцу или низ акција како би се добила максимална награда у непознатом окружењу.

Како постоји значајан број различитих приступа обради података, од којих сваки може научити доста важних информација о подацима, сложеност података не представља толико велики проблем.

При обради података у реалном времену, сваки тренутак је од значаја. Поред тачности предвиђања и прецизности, од кључног значаја су брзина и ефикасност изабране методе. Како су наведене метрике јако битан фактор у синтези оваквог система, потребно је разматрати потенцијалне изазове и потешкоће које се могу јавити у развоју њега.
Примера ради, уколико сензор прикупља податке за обраду, рецимо, сваких 200 милисекунди, потребно је конструисати систем такав да обраду тих података и прослеђивање крајњих резултата обраде може извршити пре него што му на улаз пристигну подаци из новијег мерења.

4.3 Потенцијални изазови у прикупљању и обради података у реалном времену

Изазови у прикупљању и обради података у реалном времену стварају потребу за брзим и прецизним решењима, с обзиром на константни поток информација. Латенција (кашњење), мрежни проток, синхронизација података и скалирање представљају питања која изазивају перформансе и способност система да одговори на динамичне потребе.
Додатно, разматрање изазова попут могућих грешака при обради или прикупљању података представља важан аспект. Ови изазови позивају на велику потребу за робустнијим, поузданим системима.

- **Латенција (кашњење)**
  У IoT системима, где подаци теку у реалном времену, непотребна кашњења могу утицати на учинак и тачност система. Минимизовањем латенције минимизују се одлагања и кашњења у обради или прикупљању, и тиме смањује губитак информација, и убрзава проток.

- **Мрежни проток**
  Изазови у преносу података са једног уређаја на други у оквиру IoT система могу изазвати губитак информација, и тиме недостатак информација потребних за доношење одлука у реалном времену. Битан фактор у овим системима јесте обезбеђивање адекватног мрежног протока за успешнан трансфер података са једног на други уређај у оквиру мреже.

- **Синхронизација података**
  Континуална синхронизација података између различитих уређаја и компоненти система представља изазов, поготово у IoT системима где подаци пристижу са различитих извора. Несинхронизовани подаци могу довести до нетачних анализа и непотпуности информација.

- **Скалирање**
  Систем за прикупљање и обраду података мора бити способан да се ефикасно скалира, како IoT систем расте. Скалирање са собом носи изазове попут оптимизације ресурса и управљања великом количином података.

- **Грешке при обради или прикупљању података**
  Исправност и потпуност података су кључни за избегавање грешака у процесу доношења тачних одлука. Изазови у вези са грешкама се најчешће могу јавити када су подаци динамични и долазе из различитих извора.

Сви ови изазови захтевају не само техничка решења већ и стратегије које обезбеђују робустност и поузданост у системима прикупљања и обраде података у реалном времену. Као решење свих наведених проблема, истиче се *'Edge Computing'*.

'Edge Computing' врши минимизацију кашњења, оптимизује мрежни проток и помаже у скалирању система и синхронизацији података тако што децентрализује процесе обраде података и њих саме зближава са 'изворима' података. Овај приступ омогућава развој робустнијих, ефикаснијих система који су готово отпорни на претходне изазове.

5 *'Edge Computing'* – обрада података на 'ивици'

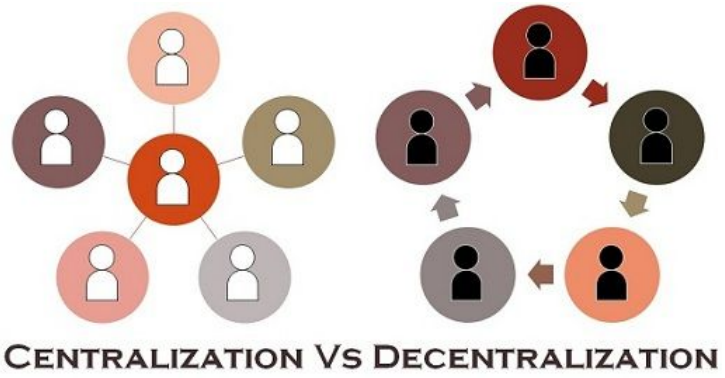
'Edge Computing' представља важну промену у методологији обраде података у *IoT* системима. Децентрализованом обрадом података могуће је 'зближити' извор са процесом обраде, и тиме првенствено знатно редуковати латенцију – што је доста важно обзиром да је потребно радити прикупљање и обраду података у реалном времену. Овим зближавањем се такође оптимизује густина саобраћаја на мрежи, како више неће сви уређаји слати податке на један централни уређај, већ на више, стратешки постављених, уређаја.

5.1 Увод у *'Edge Computing'*

Edge Computing представља иновативан приступ у обради података, где се тежи преносу процеса обраде и прикупљања података на саму 'ивицу' мреже, тамо где се подаци генеришу. Овај приступ има значајне предности, посебно у контексту Интернета ствари (*IoT*), где уређаји генеришу велики обим података у реалном времену [4].

Традиционални модел обраде података заснован је на централизованим серверима који се налазе на удаљеним локацијама. Овакав приступ може изазвати значајне латенције и проблеме у преносу података, што је неприхватљиво у контексту Интернета ствари где се захтевају брзи и реактивни системи.

Edge Computing решава ове изазове интегришући обраду података ближе извору где се подаци стварају. Примена овог концепта доприноси смањењу латенције, што значи брже и ефикасније одзиве система. Осим тога, мрежни проток се оптимизује, а синхронизација података постаје мањи изазов.
Сликом 2 дат је илустративни приказ разлика између централизованог и децентрализованог система.



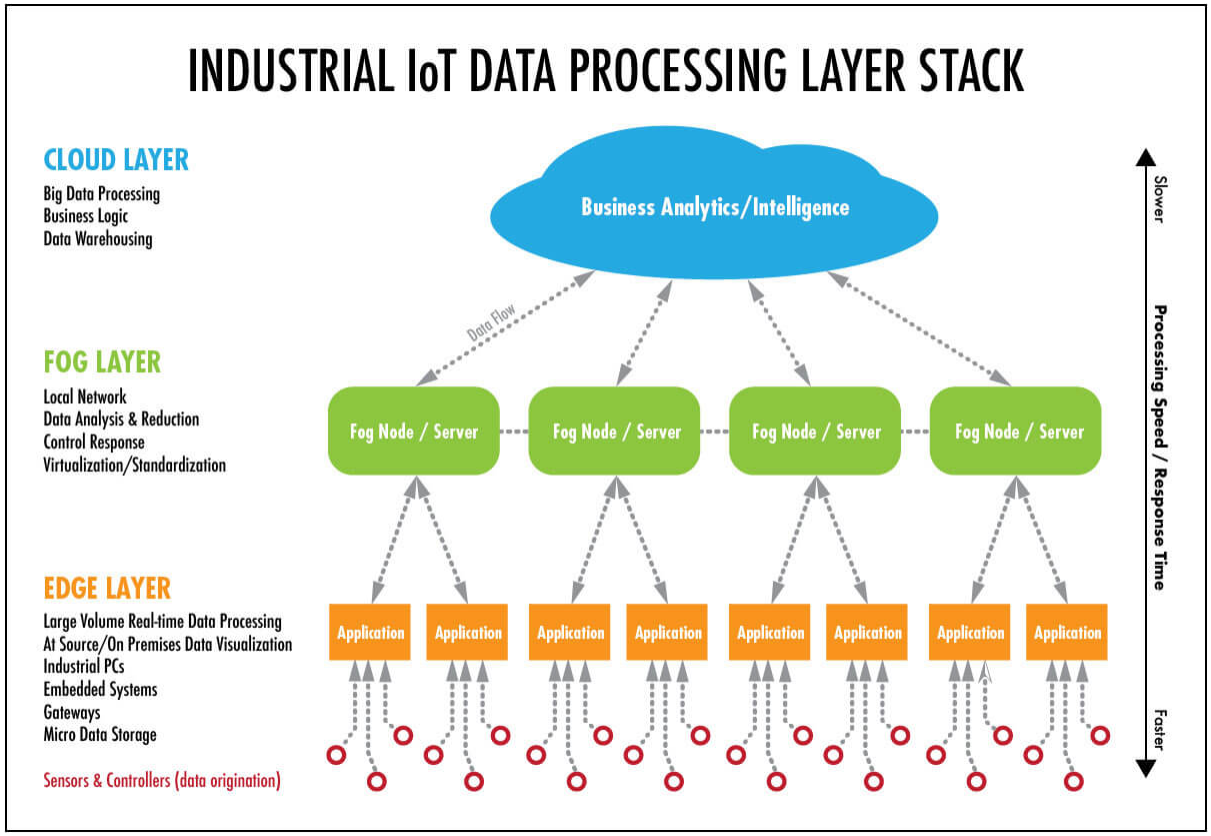
Слика 2: Пример централизације и децентрализације [5]

Edge Computing представља алтернативу алтернативу другим познатим приступима попут:

- ***Cloud Computing***
  Модел обраде и прикупљања података који се заснива на идеји да се обрада и смештање података врши на централизованим серверима, обично постављеним на удаљеним локацијама. Овај приступ омогућава висок капацитет и скалабилност, али може имати изазове као што су латенција и зависност од мрежне доступности.

- ***Fog Computing***
  Модел обраде и прикупљања података који је између *Cloud Computing*-а и *Edge Computing*-а. У овом моделу, обрада података се врши на уређајима који су ближе извору података, али не толико близу као код *Edge Computing*-а. Ово омогућава неке предности у односу на латенцију и доступност података.

Разлика у примени између *Edge Computing*, *Cloud Computing* и *Fog Computing* приступа обради и прикупљању података представљена је визуелно на слици 3.



Слика 3: Разлике у применама претходно наведене три методологије [6]

Са слике 3 може се приметити да сваки наведени приступ обради и прикупљању података има своју сврху.
Табелом 1 дате су кључне разлике између ове три методологије.

Разлике	***Cloud Computing***	***Fog Computing***	***Edge Computing***
Место обраде	Централни *Cloud* сервер	*Fog* чворови	Уређаји корисника
Кашњење	Високо	Релативно ниско	Доста ниско
Безбедност	Недовољна безбедност	Доста безбедан	Доста безбедан
Тип система	Централизован	Дистрибуиран	Дистрибуиран
Моћ обраде	Изузетна	Ограничена	Ограничена

Табела 1: Разлике између методологија

5.2 Превазилажење изазова помоћу *Edge Computing* приступа

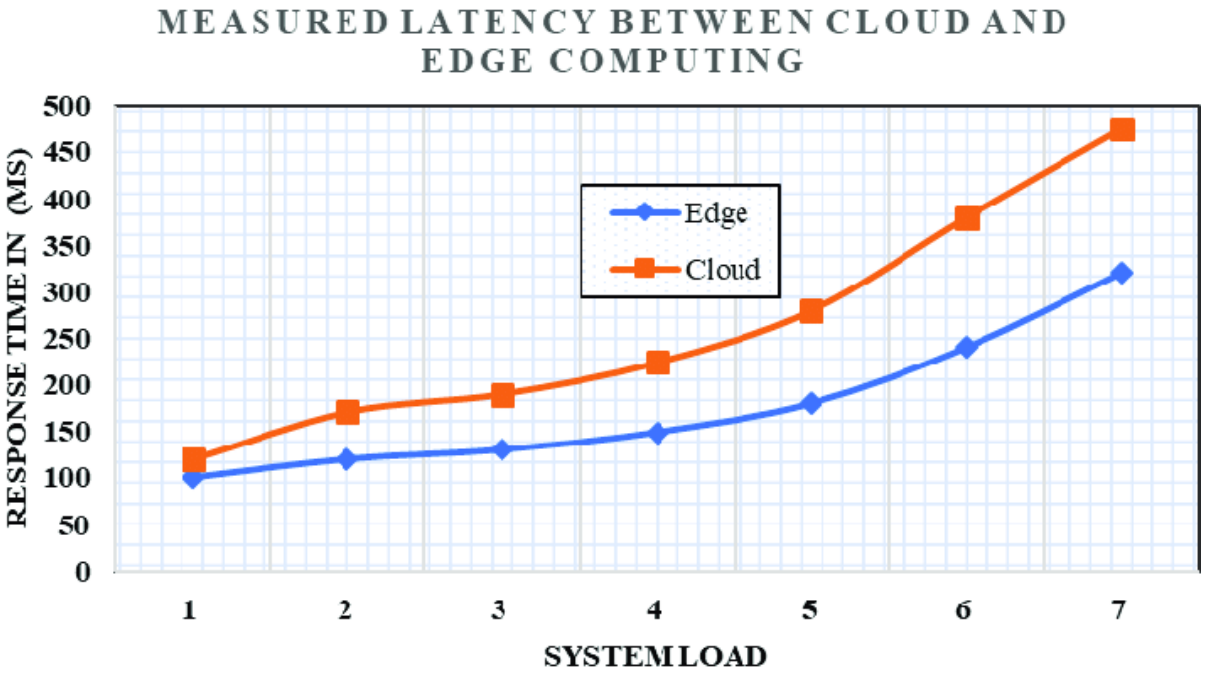
Изазови који су раније постојали у прикупљању и обради података у реалном времену могу бити адресирани интеграцијом *Edge Computing*-а.

У следећим подсекцијама, предмет истраживања ће бити како *Edge Computing* решава конкретне изазове као што су латенција, пропусност мрежа, синхронизација података и скалирање у *IoT* системима.

5.2.1 Кашњење у *Edge Computing* приступу

Кашњења у *IoT* системима које се служе *Edge Computing* приступом за обраду и прикупљање података су знатно мања него кашњења у системима који се служе *Cloud Computing* и *Fog Computing* приступима.

Сликом 4 приказан је график који указује на разлике у кашњењима између *Edge Computing* и *Cloud Computing*, у односу на оптерећење система.



Слика 4: *Edge Computing* и *Cloud Computing* кашњења [7]

Брзина одзива је као што је претходно наведено, јако важан фактор у *IoT* системима. Латенција (кашњење) може бити штетна, поготово ако подаци морају путовати до централизованог сервера и назад, до корисничког уређаја.

Edge Computing смањује наведено кашњење локализовањем процеса обраде и прикупљања података на самом уређају или близу њега. Овакво локално обрађивање података доприноси увећавању брзине одзива система, чинећи га прилагођенијим захтевима апликацијама *IoT* система [4].

5.2.2 Мрежни проток у *Edge Computing* приступу

Коришћењем дистрибуираних процеса обраде и прикупљања података, уређаји на 'ивици' мреже могу међусобно комуницирати – размењивати и обрађивати подате, без потребе за преносом истих ка централизованом серверу (као у *Cloud Computing* приступу).

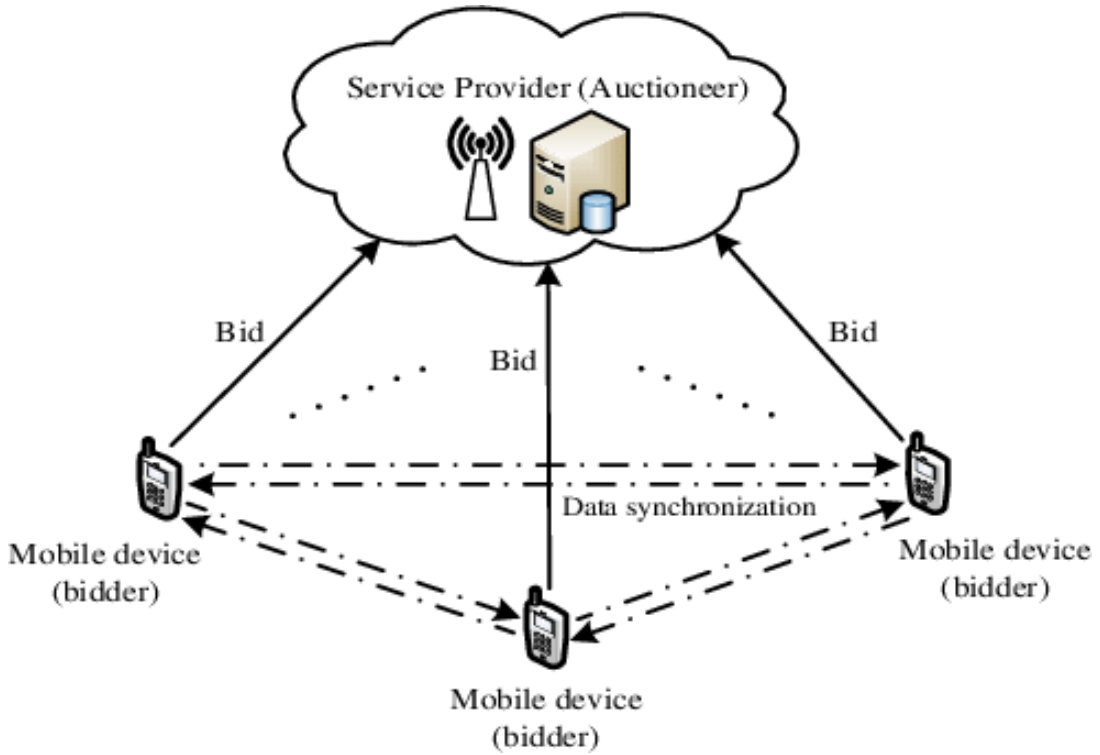
Ова оптимизација је од великог значаја, пошто се избегава гужва и велико оптерећење мреже. Децентрализација процеса обраде и прикупљања података, у овом случају, доприноси увећању ефикасности и обезбеђује брз, неоптерећени проток података кроз мрежу.

5.2.3 Синхронизација података у *Edge Computing* приступу

Један од изазова који се јавља у оквиру *IoT* система, конкретно у обради и прикупљању података са уређаја у реалном времену, јесте синхронизација података који пристижу са различитих извора.

Edge Computing омогућава локалну синхронизацију података, код које уређаји на ивици могу међусобно ажурирати податке и делити информације, што елиминише потребу за константном комуникацијом са централним сервером.

Сликом 5 приказан је дијаграм комуникације између уређаја у *Edge Computing* приступу, као и синхронизација података између њих.



Слика 5: *Edge Computing* – Синхронизација података [8]

Са слике 5 се може приметити да је могуће остварити потпуно дистрибуирану комуникацију између уређаја уз помоћ *Edge Computing* приступа. Сви уређаји могу међусобно, брзо размењивати податке.

5.2.4 Скалирање у *Edge Computing* приступу

У централизованим системима, додавањем нових уређаја умањује се његова ефикасност и јавља се захтев за увођење нових, скупих уређаја како би се оптерећење поделило.
Позивајући се на слику 2, може се приметити да, уколико у систему постоји велики број корисника у уређаја, централни уређај постаје преоптерећен.

У *Edge Computing* приступу, у којем се остварује децентрализована комуникација, додавање нових уређаја у систем не ремети и не оптерећује мрежу. Дистрибуирани модел обраде и прикупљања података којим се опслужује *Edge Computing* приступ је флексибилан и способан да се адаптира на промене у броју корисника, уређаја и у захтевима апликација (погледати слику 5).

5.2.5 Грешке при раду са подацима у *Edge Computing* приступу

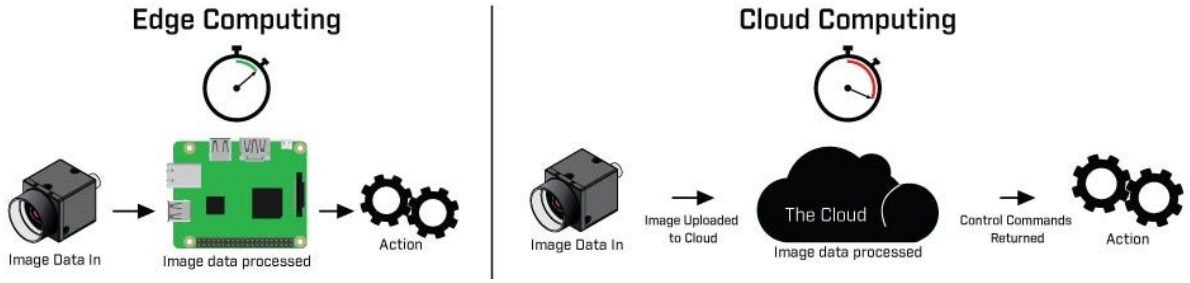
Edge Computing приступ се показао као веома ефикасан у решавању изазова и смањењу грешака при раду са подацима.

Обрада података на ивици мреже доприноси редункцији великог, непотребног протока података кроз мрежу. Само важни подаци се прослеђују централном серверу за обраду, чиме се остварује знатно умањење оптерећења мреже и вероватноће за настанак грешака у процесу преноса података, јер се они преносе у мањим количинама.
Локална синхронизација између уређаја на ивици мреже, као могућност која се јавља у оквиру *Edge Computing* приступа, је веома битан аспект у овом приступу. Ова карактеристика олакшава и убрзава комуникацију између уређаја, умањујући вероватноћу да у току синхронизације података дође до грешака.

5.2.6 *Edge Computing* и машинско учење на 'ивици'

Edge Computing приступ представља значајан корак напред у решавању изазова који су раније били приметни у прикупљању и обради података у реалном времену. Кроз интеграцију *Edge Computing*-а, могуће је адресирати и решити конкретне проблеме као што су латенција, пропусност мрежа, синхронизација података, скалирање и избегавање грешака при раду са подацима у *IoT* системима.

Слика 6 представља разлику у протоку података кроз систем коришћењем *Edge Computing*-а и *Cloud Computing*-а, респективно.



Слика 6: *Edge Computing* и *Cloud Computing* – проток података [9]

Edge Computing приступ отвара нове могућности за интеграцију са машинским учењем на ‘ивици’. Имајући могућност обраде података локално на уређајима или близу њих, *Edge Computing* отвара пут за ефикасну употребу машинског учења на уређајима који генеришу податке.

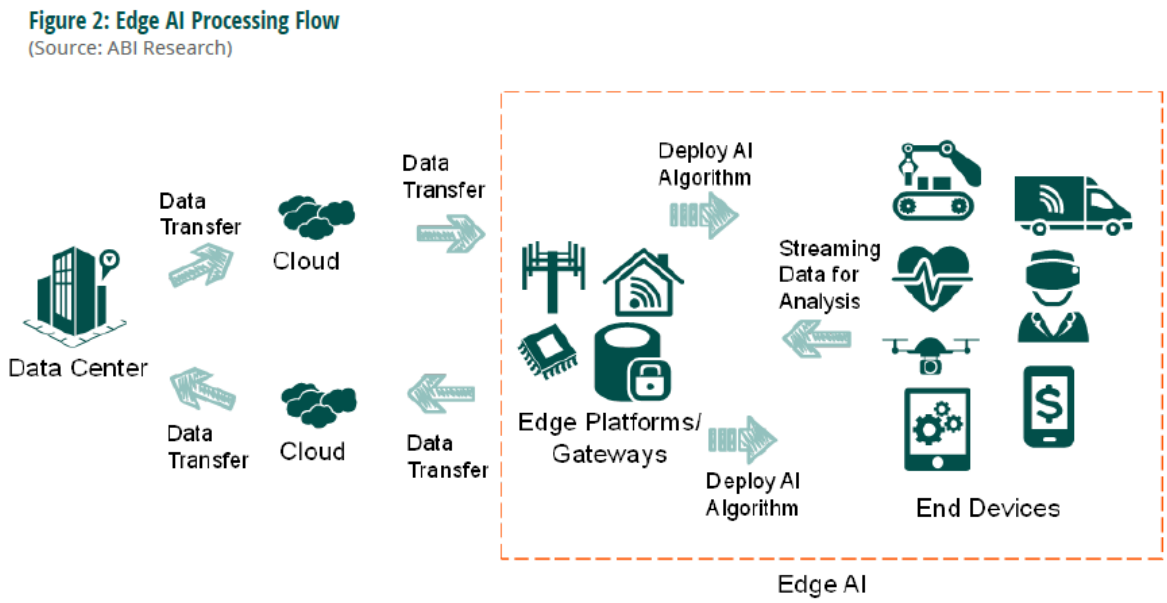
Машинско учење на ‘ивици’, познато и као *Edge Machine Learning* (*EML*), представља примену машинског учења на уређајима унутар *Edge Computing* система. Ова интеграција има значајне предности и отвара нове могућности у анализи и обради података.

С обзиром на изазове синхронизације и управљања подацима у реалном времену у *IoT* системима, *Edge Computing* у синергији са машинским учењем представља напредно и ефикасно решење. Оваква интеграција нуди брз и адаптиван систем, способан да ефикасно обрађује и анализира податке на самом месту њиховог настајања у реалном времену.

6 Машинско учење на ‘ивици’

Машинско учење на ‘ивици’ (*Edge Machine Learning*) представља напредну технику обраде података која се одвија на самим уређајима или близу њих, у оквиру *Edge Computing* приступа [3].
Овакав приступ има за циљ обављање задатака машинског учења на уређајима који генеришу податке, што има неколико предности у односу на централизоване моделе машинског учења.

Сликом 7 дат је дијаграм протока података у једном *IoT* систему који се опслужује принципом машинског учења на ивици.



Слика 7: Дијаграм система који користи машинско учење на ‘ивици’ [10]

Са слике 7 примећује се да се машинско учење примењује искључиво на ‘ивици’.

6.1 Алгоритми машинског учења на ‘ивици’

За машинско учење на ‘ивици’, често се користе алгоритми прилагођени зарад ефикасности и ограничених ресурса уређаја.

Неки од често коришћених алгоритама машинског учења у *Edge Computing* приступу укључују:

А.1 К-најближих суседа
К-најближих суседа алгоритам обично захтева мало меморије и може бити успешан у проблемима класификације на уређајима са ограниченим ресурсима. Улазни податак се класификује у неку класу на основу К инстанци које су му ‘најсличније’.

А.2 К-средњих вредности
Овај алгоритам се користи за груписање инстанци у K различитих кластера, при чему се инстанца додаје у кластер ‘најсличнији’ њој. Бира се K центроида, који представљају центре истог броја кластера, и њима се додељују подаци са најближим средњим вредностима. Алгоритам К-средњих вредности је доста брз и ефикасан, што га чини адекватним за слабије уређаје и обраду података у реалном времену.

А.3 Стабла одлучивања (*Decision Trees*)
Стабло одлучивања је алгоритам који се користи за класификацију и регресију. Он је ефикасан за моделирање неконвенционалних веза које се јављају у подацима.

А.4 Метод потпорних вектора (*Support Vector Machines - SVM*)
Метод потпорних вектора је алгоритам за класификацију који сваку инстанцу мапира као тачку у хиперравни, како би моделирао границу између класа. Критеријум одређивања граница је да су оне максимално удаљене од тачака. Овај алгоритам је врло ефикасан јер може радити са вишедимензионим подацима (доста карактеристика) и није му потребно доста примера података за обучавање.

А.5 Неуронске мреже (*Neural Networks*)
Неуронске мреже, посебно мањи модели попут метода *TinyML*, могу бити корисне за обраду података на уређајима са ограниченим ресурсима.

А.6 Случајна шума (*Random Forest*)
Случајна шума је техника за креирање ансамбла(комбинација више различитих модела, углавном са истим задатком), која комбинује слабе моделе (нпр. дрвета одлучивања) како би се постигла већа ефикасност и прецизност (учинак, генерално) предвиђања.

За успешну синтезу једног *IoT* система који се опслужује машинским учењем на ‘ивици’, неопходно је, поред адекватног пројектовања система и правилне интеграције машинског учења (добар одабир метода и алгоритама), потребно је разумети и дефинисати потенцијалне безбедносне опасности, потом применити адекватне безбедносне принципе и протоколе.

Ови принципи укључују заштиту комуникација, заштиту од неовлашћеног приступа и сигурност самих уређаја – у реалном времену.

6.2 Безбедност у систему са машинским учењем на ‘ивици’

Са широком применом машинског учења на ‘ивици’ у оквиру многих *IoT* система, безбедност постаје неизоставан аспект интеграције ових решења. Потребно је истаћи кључне безбедносне принципе и предложене мере које је потребно узети у обзир при развоју и употреби *IoT* система са машинским учењем на ‘ивици’.

Аспекте безбедности у *IoT* систему са машинским учењем на ‘ивици’ можемо поделити на следеће:

- Заштита комуникације
- Заштита од неовлашћеног приступа
- Сигурност уређаја
- Праћење и одговор на инциденте
- Етички аспекти и приватност података

6.2.1 Заштита комуникације

У *IoT* системима са машинским учењем на ‘ивици’, заштита комуникације представља основни стуб безбедности. Пренос података међу уређајима, корисницима и серверима често може садржати осетљиве информације, због чега је неопходно осигурати њихову ‘тајност’, безбедност и интегритет.

Примена енкрипције (шифровања) током комуникације, као и коришћење безбедносних протокола попут ***TLS*** (*Transport Layer Security*) и ***SSL*** (*Secure Sockets Layer*) сертификата доприноси заштити података.

Један од примера енкрипције који се користи у комуникацији је ***AES*** (*Advanced Encryption Standard*). Кључна карактеристика ***AES***-а је да користи исту дужину кључа за обе фазе криптографског процеса – енкрипцију и декрипцију. Дужина кључа у ***AES***-у може бити 128, 192 или 256 бита, и она одређује колико ће бита бити у употреби током криптографског прерађивања. Као такав, ***AES*** нуди различите нивое безбедности: ***AES-128***, ***AES-192*** и ***AES-256***.
Овај алгоритам се сматра једним од најсигурнијих и најефикаснијих шифарских алгоритама.

Заштита комуникације је поготово важна уколико уређаји преносе видео или аудио снимке, као и друге сличне информације које се могу користити за идентификацију или надгледање корисника.

Неке од мера заштита комуникације су следеће:

- Шифровање података током преноса
- Коришћење безбедних комуникационих протокола (*SSL*, *TLS*)
- Аутентификација и ауторизација уређаја приликом комуникације
- Мониторинг (праћење) мрежних потока за откривање аномалија

6.2.2 Заштита од неовлашћеног приступа

Ефикасно управљање приступом и заштита од неовлашћеног приступа представљају срж безбедности у наведеним *IoT* системима. Овај аспект обезбеђује да само овлашћени корисници и уређаји имају приступ осетљивим подацима и функционалностима.

Два веома важна концепта у заштити од неовлашћеног приступа су:

К.1 Аутентификација
Процес потврђивања идентитета корисника или уређаја

К.2 Ауторизација
Процес доделе одређених привилегија или права приступа након успешне аутентификације.

Пример: Медицински *IoT* систем, где је безбедност података кључна, аутентификација омогућава само медицинском особљу да приступи систему, док ауторизација обезбеђује да само квалификовани лекари имају привилегије приступа осетљивим медицинским информацијама.

Додатне мере заштите од неовлашћеног приступа систему могу укључивати неке од наредних мера:

- **Двострука (или вишеструка) аутентификација**
  Обезбеђује потврду идентитета корисника и уређаја коришћењем два различита метода аутентификације. На пример, комбинација лозинке и потврде преко мобилног уређаја.
  Двострука (или вишеструка) аутентификација је јако важна у случајевима када су над корисником успешно извршени напади за откривање његове лозинке попут *Brute Force* и *Phishing* напада, јер нападачу није довољна само једна потврда идентитета (лозинка или аутентификациони код) како би успешно приступио систему.

- **Праћење активности**
  Праћење и анализирање активности корисника како би се открило и благовремено спречило необично или потенцијално опасно понашање.
  Ово може укључивати употребу софтверских окидача (попут флегова) на неочекиван саобраћај ка или од неког корисника, или на предефинисан опасан или нежељен саобраћај.

- **Периодично ажурирање листе овлашћених корисника**
  Редовно освежавање и проверавање листе корисника са одређеним привилегијама приступа, како би се отклониле застареле или непотребне привилегије одређених корисника.

У оквиру једног *IoT* система са машинским учењем на 'ивици' је потребно имплементирати више слојева заштите од неовлашћеног приступа, како би систем био безбеднији.
Мере приступа које се користе се морају ефикасно примењивати, како саобраћај ка и од неког корисника не би био додатно успорен великим бројем метода које спроводе дате мере.

6.2.3 Сигурност уређаја

Сигурност уређаја је такође, од кључног значаја јер уређаји на ивици често обрађују и архивирају осетљиве податке. Коришћење безбедних микроконтролера и механизама за закључавање или шифровање нвеома је важно за сигурност уређаја. Примена ових мера омогућава спречавање неовлашћеног приступа и недозвољене модификације уређаја.

Неке од мера сигурности уређаја:

- **Коришћење безбедних микроконтролера**
  Избор микроконтролера са уграђеним безбедносним функцијама и мерама заштите помаже у спречавању напада на хардвер.

- **Закључавање или шифровање података на уређају**
  Примена јаког шифровања заштитиће податке и спречити неовлашћен приступ.

- **Могућност ажурирања система**
  Уређаји би требало да имају механизме за ажурирање система како би се исправиле откривене рањиве тачке у систему и осигурала заштита система.

- **Додатне анти-експлоататативне заштите**
  Укључивање мера заштите од преправљања системских софтверских алата доприноси спречавању покушаја напада и злоупотреба.

Поред ових мера, потребно је такође обратити пажњу на адекватно одржавање уређаја, како софтверски тако и хардверски, како не би дошло до нежељеног понашања уређаја.

6.2.4 Праћење и одговор на инциденте

Превенција је од кључног значаја за безбедност система, али и поред најбољих превентивних мера, инциденти су неизбежни. Постојање ефикасног система за праћење и одговор на инциденте (*Incident Response – IR*) врло је важно за минимизирање потенцијалних штета и обнављање нормалног рада система и уређаја што пре.

Неке од компоненти праћења и одговора на инциденте су:

- **Системи за детекцију упада (*IDS*)**
  Континуирано праћење мрежног саобраћаја и системских активности ради откривања необичних или потенцијално штетних активности.

- **Евидентирање (*Logging*)**
  Записивање и анализирање системских евидентираних података и података о активностима корисника.

- **Системи за аутоматско обавештавање**
  Аутоматизоване процедуре за обавештавање одговорног тима о потенцијалним безбедносним претњама.

- **Планови одговора на инциденте**
  Јасно дефинисани планови и процедуре за одговор на различите типове безбедносних инцидената.

- **Обучен тим за одговор на инциденте**
  Специјализован тим са обуком за брз и ефикасан одговор на инциденте.

Процес одговора на инциденте се може поделити на наредне етапе:

- **Детекција**
  Препознавање потенцијалних безбедносних инцидената.

- **Анализа**
  Истраживање и анализа природе инцидента и његових потенцијалних последица.

- **Одговор**
  Елиминација претње.

- **Обнова система**
  Процес обнављања система и постизања нормалног рада.

- **Учење**
  Побољшавање процедура за одговор на потенцијалне будуће, сличне инциденте на основу тренутног инцидента.

Ефикасан систем за праћење и одговор на инциденте значајан је у обезбеђивању брзе и ефикасне одбране против потенцијалних безбедносних инцидената и одржавању сигурности система.

6.2.5 Етички аспекти и приватност података

С обзиром на осетљивост података који се користе у алгоритмима машинског учења, етички аспекти и заштита приватности корисника су од суштинског значаја. Дизајнирање система са уграђеним мерама заштите приватности и поштовањем етичких стандарда представља важан аспект успешног развоја IoT система са машинским учењем на 'ивици'. Важно је омогућити корисницима контролу над њиховим подацима и обавештавати их о начину на који ће њихови прикупљени подаци бити употребљени [11].

Неке од мера заштите приватности и поштовања етичких стандарда су:

- **Транспарентност**
  Обезбедити јасно обавештавање корисника о томе како ће њихови подаци бити коришћени и обрађени.

- **Контрола**
  Омогућити корисницима механизме контроле над подацима који се прикупљају и користе.

- **Анонимизација**
  У случају да је могуће, употребити технике анонимизације података ради заштите идентитета корисника.

- **Сигурност података**
  Применити напредне технике шифровања и осигурати безбедност у преносу и чувању података, као што је наведено у секцији 6.2.3.

Интегрисањем ових принципа у процес развоја, системи машинског учења на 'ивици' могу успешно служити својој намени без угрожавања приватности и етичких принципа.

7 Практична примена *IoT* система са *EML*

Систем управљања паметним осветљењем – пример једног *IoT* система са *EML* 5.2.6.

Овај систем обухвата употребу сензора и метода машинског учења како би оптимизовао управљање осветљењем у реалном времену.

7.1 Опис система

Систем се састоји из наредних уређаја и елемената:

1. Сензори покрета
   (а) Способни да детектују кретање у околини.
   (б) Постављени широм објекта за који се ради систем.
2. Микроконтролери (за осветљење)
   (а) Уграђени близу групе извора светла или у сваки објекат који је извор светла (попут лампи).
   (б) Примају податке од сензора како би контролисали осветљење.
   (в) Играју улогу уређаја на 'ивици', што значи да процесирају и обрађују податке локално.
3. Бежична мрежа
   (а) Повезује сензоре и микроконтролере.
4. Кориснички интерфејс или апликација
   (а) Омогућава корисницима потпуну контролу и могућност прилагођавања осветљења.
   (б) Праћење корисничких преференција.

7.2 Улога машинског учења у систему

1. Локална обрада података
   (а) Употреба *LTSM* методе дубоког учења, која на основу историјских података сензора покрета предвиђа шаблон кретања људи и тиме коју просторију или регион је потребно осветлити.
2. Доношење одлука у реалном времену
   (а) Систем обраде података на ивици доприноси брзини одзива система, и тиме процес предвиђања брже долази до одлуке.
3. Сигурност
   (а) Подаци о коришћењу осветљења и обавештења о корисницима обрађују се локално.
   (б) Смањен ризик од излагања података преко мреже.

7.3 Рад система

1. **Инсталација система и пуштање у рад**
   По инсталацији система за управљање паметним осветљењем, први корак је инсталирање сензора покрета на стратешким местима. Ови сензори се подешавају у складу са параметрима као што су осетљивост и домет, како би обезбедили ефикасно праћење покрета у околини. Затим, микроконтролери који играју улогу уређаја на 'ивици' се уграђују у сваку лампу или вештачки извор светлости и програмирају за пријем и обраду података са сензора.

   Путем бежичне мреже, врши се повезивање сензора и микроконтролера. Кориснички интерфејс и апликације се инсталирају на уређајима за контролу и праћење осветљења, омогућавајући корисницима да контролишу и прилагођавају осветљење према својим жељама.

2. **Обучавање система – примена техника машинског учења**
   Процес обучавања система почиње прикупљањем података о кретању и коришћењу осветљења. Систем прати активности сензора и команде корисничког интерфејса. Прикупљени подаци се затим користе за тренирање алгоритама машинског учења на микроконтролерима.

   Алгоритам *LTSM* [1] (*Long Term Short Memory*), се извршава на микроконтролерима. Подаци о коришћењу осветљења и корисничким преференцама се обрађују локално, што смањује ризик од излагања података преко мреже.

3. **Систем у раду**
   Када сензори детектују покрет, информације се шаљу микроконтролерима. *LTSM* неуронска мрежа обрађује информације и доноси одлуку о најприкладнијем осветљењу (за групу светла за коју је задужен) на основу анализе и предвиђања.

   Локално прилагођавање осветљења и обрада података машинским учењем се извршавају без прослеђивања на централни сервер. Овај *IoT* систем користи машинско учење на 'ивици' за локалну обраду и прикупљање података, што доводи до брзих и ефикасних одлука у вези са управљањем осветљењем. Одлуке машинског учења се извршавају на самом уређају, што доприноси брзини, ефикасности и повећању безбедности података.

Овај систем за управљање паметним осветљењем представља пример савремене практичне примене и синтезе *IoT* система са машинским учењем на 'ивици'. Коришћење сензора покрета, микроконтролера и алгоритама машинског учења, ова технологија обезбеђује ефикасно и интелигентно управљање осветљењем у реалном времену. Овакви системи представљају следећи корак у еволуцији паметних окружења и доприносе стварању интелигентних и енергетски ефикасних јавних или приватних објеката.

[1] *Long Short-Term Memory (LSTM)* је тип рекурентних неуронских мрежа (*RNN*) који је дизајниран да реши проблем временски зависних података. У контексту машинског учења за обраду података са сензора покрета у системима паметног осветљења, овај тип неуронске мреже игра важну улогу у анализи и одлучивању на основу претходних и текућих података.

8 Закључак

У оквиру овог истраживања дубоко су проучени принципи, технике и примене машинског учења у оквиру Интернета ствари (IoT). Уводећи концепт Интернета ствари, истакнут је његов значај и потенцијал у модерном друштву. Заједно са методама машинског учења, ова област представља кључни елемент у преображају начина на који људи са околином и технологијом.

Разматрајући предности употребе метода машинског учења у IoT системима, истакнуто је како алгоритми машинског учења омогућавају аутоматску анализу и одлучивање на основу података, што значајно унапређује ефикасност и перформансе система.

Детаљним увидом у интеграцију метода машинског учења у IoT системе, издвојени су различити типови података као и где се могу пронаћи, и методе учења са примерима. Наведени су потенцијални изазови у прикупљању и обради података у реалном времену, као и како их превазићи потенцијалних помоћу напредних метода машинског учења.

Као предлог решења изазова, дефинише се појам *Edge Computing* принципа. Фокус овог принципа је обрада и прикупљање података на 'ивици', што значајно побољшава учинак система, убрзава одзив и смањује кашњења. Овај приступ се може успешно интегрисати са методама машинског учења, како је овај приступ врло подударан са потребама машинског учења, и обрнуто. Дефинишу се конкретне предности овог принципа у односу на друге, у општем случају као и у случају интеграције са машинским учењем.

Истраживањем појма машинског учења на 'ивици', као и његове алгоритме и безбедносне аспекте, долази се до закључка како локална обрада података и примена одговарајућих алгоритама доприносе брзим и сигурним одлукама. Наводи се како се у систему са машинским учењем на 'ивици' могу успешно решити изазови попут заштите комуникације и од неовлашћеног приступа, сигурности самих уређаја, праћења и брзог одговора на инциденте и етички аспекти, као и приватност података.

Како би се, поред теоријског дела теме, продискутовао и практичан део, дат је пример једног IoT система са машинским учењем на 'ивици'. Конкретно, практичан пример представља развој система за управљање паметним осветљењем. У оквиру те секције, наведени су и објашњени потребни делови система, дат алгоритам машинског учења за дати проблем као и његове предности у овом случају. Поред описа система, детаљно је обрађен и сам рад система, од инсталације, припремања алгоритама машинског учења система до стабилног система у радном режиму. Овај систем илуструје успешну интеграцију технологија наведених у оквиру ове теме, и то у реалном окружењу.

Потребно је истаћи снажан утицај који IoT системи, са интегрисаним машинским учењем на 'ивици' имају на друштво и индустрију, као и неограничене прилике које ти системи пружају за будућност. Уколико се може претпоставити да сваки уређај може постати паметан и ефикаснији са интеграцијом у IoT систем, може се гарантовати да се додатном употребом метода машинског учења ефикасност и употребљивост таквих уређаја значајно увећава.

Даља истраживања у оквиру синергије ове две технологије отвориће нове перспективе и могућности развоја у свим делатностима и наукама. Претпоставља се да ће се ове две технологије међусобно унапређивати, доприносећи напретку и иновацијама које могу, потенцијално, обликовати будућност.

Литература

[1] *What is the internet of things (IoT)?* Преузето 9. Јануара 2023. URL: https://www.ibm.com/topics/internet-of-things.

[2] *Tech 101: Internet of Things*. Преузето 4. Јануара 2023. URL: https://businesstech.bus.umich.edu/uncategorized/tech-101-internet-of-things/.

[3] M. G. Sarwar Murshed и др. „Machine Learning at the Network Edge: A Survey". У: *ACM Comput. Surv.* 54.8 (нов. 2021.). ISSN: 0360-0300. DOI: 10.1145/3469029. URL: https://doi.org/10.1145/3469029.

[4] Mehtab Alam и Ehtiram Khan. „Edge Computing and its Impact on IoT". У: (јан. 2021.). DOI: 10.6084/m9.figshare.14369642.

[5] *Difference Between Centralization and Decentralization*. Преузето 4. Јануара 2023. URL: https://keydifferences.com/wp-content/uploads/2015/05/Centralization-Vs-Decentralization.jpg.

[6] *Cloud, Fog and Edge Computing - The Difference*. Преузето 6. Јануара 2023. URL: https://www.winsystems.com/wp-content/uploads/2017/12/cloud-fog-edge_infographic.jpg.

[7] Manjur Kolhar. *A Three Layered Decentralized IoT Biometric Architecture for City Lockdown during COVID-19 Outbreak*. Преузето 6. Јануара 2023. URL: https://www.researchgate.net/profile/Manjur-Kolhar/publication/344218742/figure/fig3/AS:934938396336128@1599918092606/Latency-of-Cloud-and-Edge-computing-of-Application-and-database-server.png.

[8] Ziyao Liu и др. *A Survey on Applications of Game Theory in Blockchain*. Преузето 7. Јануара 2023. URL: https://www.researchgate.net/figure/An-example-of-the-system-model-of-edge-computing-in-mobile-blockchain-network-The-mobile_fig5_331429224.

[9] Bharath Raj. *Deep Learning on the Edge*. Преузето 7. Јануара 2023. URL: https://towardsdatascience.com/deep-learning-on-the-edge-9181693f466c.

[10] Yih-Khai Wong. *How the Edge Enables Groundbreaking AI Applications*. Преузето 7. Јануара 2023. URL: https://www.abiresearch.com/blogs/2023/03/24/edge-ai-applications/.

[11] Dr. Attlee M. Gamundani и Dr. Serge Stinckwich. „Ethical Issues in ML and IoT". У: *ICTP Workshop on TinyML* (окт. 2021.).