

# Komplex, elosztott rendszerek viselkedésének elemzése

(Behaviour analysis of complex, distributed systems)

Kertész Attila

*Szegedi Tudományegyetem  
Természettudományi és Informatikai Kar  
Informatikai Intézet  
Szoftverfejlesztés Tanszék*

MTA Doktori Értekezés Tézisei

2023

## Contents

|  |           |
|--|-----------|
| <b>1. A kutatás területei és módszerei</b>                               | <b>1</b>  |
| <b>2. Az értekezés tézisei</b>   | <b>2</b>  |
| 1. tétiscsoport: Felhő föderációk vizsgálata . . . . .                   | 2         |
| 2. tétiscsoport: IoT-Felhő rendszerek vizsgálata . . . . .               | 5         |
| 3. tétiscsoport: IoT-Köd-Felhő rendszerek vizsgálata . . . . .           | 7         |
| 4. tétiscsoport: IoT-Blokklánc-Köd-Felhő rendszerek vizsgálata . . . . . | 9         |
| <b>3. Az eredmények hasznosulása</b>                                     | <b>12</b> |
| <b>A Szerző hivatkozott publikációi</b>                                  | <b>13</b> |
| <b>További hivatkozott közlemények</b>                                   | <b>17</b> |

## 1. A kutatás területei és módszerei

Az elmúlt évtizedben a számítási felhők (Cloud Computing [37]) széles körben elterjedtek, és napjainkra megbízható megoldást nyújtanak az információ- és kommunikációtechnológia (IKT) területén felmerülő számos problémára, skálázható, virtualizált adattárolási és számítási szolgáltatások alkalmazásával.

A korábbi, számítási gridekkel ellentétben, a felhő rendszerek kifejlődésében úttörő szerepet játszottak az üzleti célú szolgáltatók és cégek, melyek a rugalmasan kialakítható virtuális infrastruktúrák alkalmazásából terveztek profitálni. A publikus felhő szolgáltatók és a különböző középréteg implementációk közötti együttműködés elősegítésére felhő föderációkat dolgoztak ki és hoztak létre. A föderációban részt vevő szolgáltatók egymás erőforrásait az időszakosan megnövekedő ügyfélkörük folyamatos kiszolgálása miatt tervezték igénybe venni, nyílt standard interfészeket keresztül, szolgáltatási szerződések kötésével.

A hagyományos, főként web szolgáltatásokat biztosító számítási igények mellett egy új technológia támasztott újabb kihívásokat a felhő rendszerek számára: a Dolgok Internete (IoT, azaz Internet of Things [39]). A CERP-IoT európai klaszter már 2010-ben előjelezte az önműködő képességekkel rendelkező okoseszközök Interneten történő nagy számú megjelenését, jelentős adatforgalommal, valamint számítási és adattárolási igényekkel, melyeket nagyrészt felhő szolgáltatások biztosítanak. Az elmúlt években az online elérhető IoT eszközök száma meghaladta a százmilliárdos nagyságrendet, mely előidézte az IoT-Felhő rendszerek kialakulását.

Az IoT alkalmazások robbanásszerű terjedése újabb kihívásokat is magával hozott. A végfelhasználók kiszolgálása távoli felhő erőforrásokkal egyre lassabban valósult meg, mely életre hívta a Köd Számítások (azaz Fog Computing [40]) megjelenését: a kritikus adatok tárolását és a gyakori alkalmazáskomponensek végrehajtását végezhetjük a felhasználóhoz közeli erőforrásokon, rövidebb válaszidőt elérve. Ezt a módszert is alkalmazva IoT-Köd-Felhő rendszereket alakíthatunk ki, melyek már képesek lehetnek a legtöbb okos alkalmazás hatékony kiszolgálására.

Az adattárolási és feldolgozási igényeken túl, biztonsági, bizalmi és magánszférevédelmi aggályok is megjelennek ezekben a rendszerekben és alkalmazásaikban. Ezen problémák jelentős részére megoldást adhatnak a Blokklánc (Blockchain [42]) rendszerek, melyek megmásíthatatlan, teljesen elosztott adattárolást nyújtanak. Alkalmazásukkal eljutunk a legbővebb, IoT-Blokklánc-Köd-Felhő rendszerek kialakulásához.

Természetesen az ilyen komplex rendszerek tervezése, megvalósítása és működtetése számos kihívással és megoldandó problémával rendelkezik. Kutatásaim fókuszában a fent megnevezett és röviden bemutatott technológiák együttes alkalmazásának vizsgálata állt. Disszertációmban számos módszert, algoritmust és szimulációs eszközt mutatok be, melyek lehetővé teszik ezen technológiák közös alkalmazásával előálló komplex rendszerek tervezésének és viselkedésének elemzését.

Terjedelmi korlátok miatt, disszertációmban a PhD fokozatom megszerzése óta eltelt valamivel több, mint tíz év tudományos eredményeinek csak egy részét tudtam négy téziscsoportba rendezve bemutatni. A szakterület elvárásait kielégítő gondos és részletes kiértékelések és validációk csak a vonatkozó közleményekben található meg.

Az első téziscsoport a felhő föderációk kialakításával és működtetésével kapcsolatos módszereket foglalja össze, melyek nagy része közvetlenül a PhD fokozatszerzésemet követő években, nemzetközi együttműködések keretében született meg.

A második, harmadik és negyedik téziscsoportban sorban az IoT-Felhő, IoT-Kód-Felhő, majd az IoT-Blokklánc-Kód-Felhő rendszerek modellezésével és elemzésével kapcsolatos eredményeket foglaltam össze. Ezen téziscsoportok eredményeinek elérésében fontos szerepe volt Pflanzner Tamás, Márkus András és Baniata Hamza volt doktoranduszaimnak, jelenlegi tanszéki kollégáimnak. Ezen téziscsoportokhoz kapcsolódó eredmények nagy része a Szegedi Tudományegyetem Szoftverfejlesztés Tanszékén belül létrehozott kutatócsoportom munkájának keretében született, BSc és MSc hallgatók témavezetésével kiegészítve.

## 2. Az értekezés tézisei

Az alábbiakban összefoglalom a disszertációmba beválogatott, a PhD dolgozatom megvédése óta eltelt 12 évben elért tudományos eredményeimet. A négy téziscsoportba rendezett eredmények tömör bemutatása mellett megadom az alátámasztó közleményeket, valamint az együttműködések keretében végzett kutatásoknál ki térek a partnerek hozzájárulására is.

### 1. téziscsoport: Felhő föderációk vizsgálata

- 1.1. Kidolgoztam egy föderált felhő vezérlő módszert és egy integrált felhő monitorozó megoldást, melyekkel hatékony felhő választást valósíthatunk meg alkalmazások futtatásához.

A felhő föderációk kezelésének vizsgálatához egy föderált felhő vezérlő módszert dolgoztam ki (Federated Cloud Management (FCM) [24]), melyben a résztvevő felhő rendszerek együttműködését a szakirodalomban alkalmazott bilaterális erőforrás bérlet helyett, egy magasszintű brókerezési (meta-brókezerési) megközelítéssel javasoltam megoldani. Ez a módszer bár nem gátolja a részt vevő felhő szolgáltatók egymás közti erőforrás megosztásokat, az ilyen tevékenységek a magasabb, vezérlő szinten rejtve maradnak. A megközelítés előnye, hogy a föderáció létrehozásához nincs szükség az alacsonyabb, szolgáltatói szinten újabb szoftverek telepítésére,

közös interfészek megvalósítására. A föderáció kialakításának logikája magasabb szintre kerül, nem szükséges standardokat bevezetni az együttműködés biztosításához, amely sok üzleti szolgáltató esetében nem támogatott. Az FCM architektúra kialakításának vizsgálatait és módszereit vezetésemmel, hazai együttműködés keretében az MTA SZTAKI-ban Kecskeméti Gáborral és korábbi kollégáimmal együtt végeztük. A meta-brókezerési megoldás az alacsonyabb szintű felhő szolgáltatások kiválasztását monitorozott erőforrás terheltségi információk alapján végzi, melyhez virtuális gépekbe integrált monitorozó megoldást dolgoztunk ki privát és publikus felhőkhöz [11]. Az infrastruktúra teljesítményét tükröző monitorozott információkat a UPC-ben fejlesztett SALMon keretrendszerrel dolgoztuk fel és értékeltük ki Xavier Franch (UPC, Barcelona, Spanyolország) professzorral és kutatótársaival együttműködésben, a nemzetközi S-Cube EU FP7 projektben.

- 1.2. Kidolgoztam egy rendszerezést felhő föderációk és IoT-Köd-Felhő rendszerek adatvédelmi problémáinak csoportosítására, mely iránymutatásként szolgál a jogi felelősség meghatározásában.

A felhő föderációkban keletkező felhasználói adatok védelméhez, és a felhasználók magánszféra-védelemhez fűződő alapjogainak biztosítására világszerte adatvédelmi szabványozásokat vezettek be. Az Európai Unióban kezdetben az Adatvédelmi irányelv (DPD), majd 2018-tól a GDPR tölti be ezt a szerepet. Kapcsolódó kutatásainkban először a DPD alkalmazhatóságát vizsgáltuk meg felhő föderációk különféle használati eseteiben [22, 25], a főbb kapcsolódó szerepkörök beazonosításával, és az esetek kategorizálásával.

A technológiai fejlődés következtében megjelenő új módszerek, főként a kód számítások, a Dolgok Internete és a Mesterséges Intelligencia alkalmazása újabb kihívásokat és megvizsgálandó eseteket teremtett. Ezek alapján újabb használati eseteket azonosítottunk be és vizsgáltunk meg az IoT-Köd-Felhő rendszerekben adatvédelmi megfelelés szempontjából [28]. Eredményeink azt mutatták, hogy sokszor tapasztalható dinamikus szerepkörváltás (adatfeldolgozó és adatkezelő), mely fontos tényező a felelősség meghatározásánál. Emellett azt állapítottuk meg, hogy amint a rendszerek komplexitása növekszik, azaz egyre több technológiát alkalmaznak, úgy gyengül a felhasználók ráhatása az adatkezelési folyamatokra, melynek következtében nagyobb felelősség hárul a szolgáltatókra. Ezekben a kutatásokban a jogi vonatkozásokat az SZTE Jogi Karáról Váradi Szilvia segítségével vizsgáltuk meg.

- 1.3. Pliant-alapú optimalizációs algoritmusokat dolgoztam ki felhő föderációk adatközpontjainak energiahatékony működtetésére. A módszert a CloudSim szimulátor kiterjesztésével implementáltam és értékeltem ki.

A felhő föderációk energiafogyasztásának és szén-dioxid kibocsátásának csökkentéséhez olyan módszert dolgoztunk ki, mely az FCM architektúra alsó, felhő brókerezési rétegében hoz döntést az alkalmazások végrehajtási helyéről. Dombi József Dániel kollégám segítségével olyan Pliant rendszert alkalmazó döntési stratégiát dolgoztunk ki, mely az adatközpontokban elérhető virtuális gépeket kiszolgáló processzorok terheltségét és energiafogyasztási modelljét veszi figyelembe az alkalmazás komponensek gépekre történő allokálásához [9]. A kidolgozott módszert a CloudSim felhő szimulátor kiterjesztésével értékeltük ki. Az elvégzett kísérletek megmutatták, hogy a Pliant algoritmus képes a végrehajtási idő és az energiafogyasztás együttes csökkentésére, valamint arányuk az algoritmus paraméterezésével a felhasználói igényeknek megfelelően finomhangolható.

1.4. Kidolgoztam egy meta-brókerezésre épülő, SLA-alapú szolgáltatás virtualizációs megoldást felhő föderációk számára.

A szolgáltatásokat funkcionális képességeikkel és szolgáltatásminőségi tulajdonságaikkal jellemezhetjük. A szolgáltatásminőség (Quality of Service) számos tulajdonságot foglal magába (pl. rendelkezésre állás, biztonság, válaszidő), melyek fontos szerepet játszanak egy adott szolgáltató megítélésében. A felhő rendszerekben nyújtott szolgáltatásokra vonatkozóan szolgáltatásminőségi modelleket vizsgáltunk meg, és olyan metamodelleket határoztunk meg, melyek képesek a szakirodalomban fellelhető különféle szolgáltatásminőségi attribútumok kategorizálására [14]. Ezt a kutatást Kyriakos Kritikós (ICS-FORTH, Kréta, Görögország) vezetésével, több partnerrel együtt az S-Cube EU FP7 projekt keretében végeztük. Az elemzés eredményeképpen azt állapítottuk meg, hogy egy olyan új leírnyelv lenne szükség, mely képes a teljes szolgáltatási életciklust érintő szolgáltatási szint szerződések (Service level agreement, SLA) kifejezésére.

Ezt a kutatási irányt folytatva Ivona Brandic-csal (TUW, Bécs, Ausztria) együttműködésben vizsgáltuk meg az SLA-k autonóm számítási módszerekkel történő alkalmazhatóságát [10]. Vezetésemmel egy olyan holisztikus architektúrát dolgoztunk ki az SLA-alapú szolgáltatás virtualizáció (SLA-based Service Virtualization, SSV) üzleti célú megvalósításához, mely szerződés tárgyalási, brókerezési és szolgáltatás telepítési megoldásokra épít.

Ebben a téziscsoportban felsorolt kutatási eredmények eléréséhez számos nemzetközi együttműködésben vettem részt, többek között a következő neves kutatókkal: Ivona Brandic (TUW, Bécs, Ausztria), Xavier Franch (UPC, Barcelona, Spanyolország), Vlado Stankovski (UNILJ, Ljubljana, Szlovénia). Az 1. téziscsoportéhoz tartozó publikációk: [8], [9], [10], [11], [13], [14], [22], [24], [25], [28].

## 2. téziscsoport: IoT-Felhő rendszerek vizsgálata

- 2.1. Mishra Biswajeebannal közösen kiértékeltek és osztályoztuk az MQTT protokollt alkalmazó üzenetbrókereket.

Az IoT rendszerekben számos üzenetküldési protokoll használatos, melyek közül az MQTT, CoAP, AMQP és a HTTP a leggyakrabban használtak. Mishra Biswajeebannal közösen részletes irodalomkutatást végeztünk ezen a területen [19], és megállapítottuk, hogy az MQTT a legelterjedtebb az IoT rendszerekben. Az MQTT-t alkalmazó üzenetkezelő megoldásokat részletesebben megvizsgálva csoportosítottuk őket az elérhető nyílt forráskódjuk, valamint tervezési, megvalósítási és biztonsági jellemzőik alapján. Ezek közül a 6 legígéretesebb üzenetbróker teljesítményteszteléssel is megvizsgáltuk, lokális fizikai, és felhős infrastruktúrák alkalmazásával [20]. A mérési eredményeket három kategória alapján csoportosítottuk: (i) nem-skálázódó brókerek üzenetfeldolgozási képessége teljes CPU terheltség alatt, (ii) skálázódó brókerek üzenetfeldolgozási képessége teljes CPU terheltség alatt, és (iii) az összes bróker összehasonlítása késleltetés szempontjából. A kiértékelési eredmények alapján a Mosquitto MQTT bróker nyújtotta átlagosan a legjobb teljesítményt.

- 2.2. Megterveztem egy módszert IoT-Felhő rendszerek részleges szimulációs vizsgálatára. A módszer alapján kidolgoztuk és kiértékeltek a MobIoTSim, mobilis IoT szimulátort Pflanzner Tamással, mely képes valós szenzor adatokat generálni és küldeni valós hálózati környezetben felhős szolgáltatásoknak.

Napjainkban a hatalmas számú új eszköz interneten való megjelenése az IoT paradigma megszületését eredményezte. Az IoT rendszerekkel foglalkozó szakemberek több kihívással is küzdenek: szenzorokat és okoseszközöket kell vásárolniuk, meg kell tervezniük és meg kell valósítani az azokat kezelő infrastruktúrát, IoT alkalmazásokat kell fejleszteniük, tesztelniük kell ezeket az alkalmazásokat, ki kell értékelniük, végül finomhangolni kell azokat.

Az újonnan felmerülő igényekre a felhő szolgáltatók is felfigyeltek és új, IoT-specifikus szolgáltatásokat kezdtek nyújtani. A 2018-ban végzett irodalomkutatásunkban 20 tipikus IoT alkalmazást azonosítottunk be és vizsgáltunk meg [21]. Ezen alkalmazások alapján három osztályozási kategóriát határoztunk meg IoT alkalmazások követelményelemzése szempontjából: okos otthon, okos város és okos régió. Elemzésünk eredményeire építve terveztem meg egy olyan szimulációs módszert, mely képes valós IoT eszközök viselkedését modellezni, miközben valós átjáró (gateway) szolgáltatásokkal kommunikál. Ez a módszer a hagyományos szimulációs megoldásokhoz képest részleges szimulációt valósít meg. A módszer alapján dolgoztuk ki a MobIoTSim IoT eszközszimulátort [12], melynek implementációját

Pflanzner Tamás végezte. A generált adatokat a szimulátor az MQTT protokollon keresztül valós időben küldi el a felkonfigurálásának megfelelően. Rob van der Mei (VU, Amszterdam, Hollandia) vezetésével, több partnerrel együtt az ACROSS EU COST Akció keretében megvizsgáltuk, hogy az IoT alkalmazások kiszolgálását miként segíthetik a felhő föderációk nagyobb skálázhatóság és flexibilitás biztosításával [23], és ebben a MobIoTSim milyen szerepet játszhat.

- 2.3. Kidolgoztunk egy általános felhős átjáró (gateway) szolgáltatást Pflanzner Tamással, mely képes IoT eszközök hatékony kezelésére és adatainak vizualizálására. Kidolgoztuk a módszer specializált változatát, az IoLT átjáró alkalmazást, mely képes üvegházi növények távoli monitorozására.

A szimulátort egy keretrendszerbe foglaltuk, mely képes az Interneten elérhető adattárakból és nyilvános adatokból, valós IoT szenzor adatokat automatizált módon gyűjteni és szűrni (SUMMON - Smart city Usage data Management and Monitoring) [34]. Az így előállított adatok (trace-ek) betölthetők a MobIoTSim szimulátorban és lejátszhatók. A szimulátor kiértékeléséhez kidolgoztunk egy privát átjáró (gateway) szolgáltatást [35], mely képes több száz (adott esetben szimulált) IoT eszköz együttes kezelésére. Az átjáró webes felülettel rendelkezik, az IoT üzeneteket JSON formátumban kezeli, és képes kétirányú kommunikációra a Mosquitto MQTT bróker alkalmazásával, a MobIoTSim-mel és valós eszközökkel is. Az átjáró implementációját Pflanzner Tamás végezte. Az általános gateway használhatóságát skálázhatósági vizsgálatokkal igazoltuk. A Docker konténerbe csomagolt átjárót az IBM Cloud felhőbe telepítve értéktől ki többféle alkalmazás típussal (generált termosztát és valós, betöltött OpenWeatherMap archívum adatok alapján), több száz eszköz csoportos kezelésével. Az eredmények azt mutatták, hogy bár az időjárási adatokat tartalmazó nagyobb méretű üzenetek nagyobb processzor terheltséget idéztek elő, a MobIoTSim hasonlóan képes volt megbízhatóan kezelni az eszközöket.

Az okos agrárium egy gyorsan növekvő terület az okos rendszereken belül. Az IKT fejlődésének következtében az IoT technológiák alkalmazása segíti ezt a területet is, mely megoldásokat megfizethető fenotipizálásnak (affordable phenotyping) neveznek. Ehhez kapcsolódóan az Élő Dolgok Internete hazai GINOP projektben Vass Imrével és SZBK-s kollégáival kidolgoztuk az IoLT Okos Cserép megfizethető fenotipizálási platformot [27], amely képes kisméretű növények növekedésének távoli megfigyelésére egy átlagos üvegházi környezetben. Az ilyen okos cserepekből álló klaszterek kezeléséhez az IoLT Okos Cserép Gateway alkalmazást dolgoztuk ki az általános gateway fejlesztési eredményeinkre építve. Ezt követően elvégeztük ennek a specializált gatewaynek a szimulációs skálázhatósági vizsgálatait, mellyel megmutattuk helyes működését valós környezetben.



Ebben a téziscsoportban felsorolt kutatási eredmények eléréséhez számos nemzetközi együttműködésben vettem részt, többek között a következő neves kutatókkal: Rob van der Mei (VU, Amszterdam, Hollandia) and Burkhard Stiller (UZH, Zürich, Svájc). A 2. téziscsoportához tartozó publikációk: [12], [19], [20], [21], [23], [27], [34], [35].

### 3. téziscsoport: IoT-Köd-Felhő rendszerek vizsgálata

- 3.1. Megterveztünk egy taxonómiát Márkus Andrással IoT-Köd-Felhő rendszerek szimulációs megoldásainak osztályozásához, melynek segítségével elemeztük és csoportosítottuk a létező szimulátorokat.

Az elosztott számítási megoldások felhőket követő paradigmáját a Köd Számítá-sok kialakulása (Fog Computing - FC) jelenti [41], melyben a hálózat szélén, a felhasználókhöz közel, elhelyezkedő csomópontok egy ún. ködbe csoportosulnak. Alkalmazásukkal az adatelemzési és feldolgozási feladatokat kisebb késleltetéssel és magasabb szolgáltatásminőséggel végezhetjük el, mint a távoli felhős erőforrások igénybevételével. A használatukkal előálló IoT-Köd-Felhő rendszerek újabb kihívásokat támasztanak a hatékony rendszervezést illetően, vizsgálatukhoz pedig elengedhetetlen szimulációs környezetek alkalmazása. Kutatásom folytatásaként a kapcsolódó szimulátorokat kezdtem el elemezni, és Márkus András segítségével egy részletes irodalomkutatást követően megterveztünk egy taxonómiát az IoT, köd és felhő rendszerek nagy részét lefedő szimulátorok osztályozására [15]. A szakirodalomban is fellelhető csoportosítási módszerek mellett egy új, szoftver metrikákon alapuló elemzést is végeztünk ebben a munkában, mely a használhatóságot és megbízhatóságot hivatott jellemezni.

A tulajdonság-alapú osztályozási vizsgálatok mellett futtatási kísérleteket is végeztünk a legelterjedtebb iFogSim, és az általunk fejlesztett DISSECT-CF-Fog szimulátorokkal [26]. A kísérleti eredmények igazolták a metrikák által felfedett jellemzőket, és megerősítették DISSECT-CF-Fog hatékonyabb alkalmazhatóságát nagyobb skálájú vizsgálatokhoz.

- 3.2. Megterveztem egy bővíthető modellt IoT eszközök, köd erőforrások és szolgáltatói árazási sémák leírására. Kidolgoztuk a modellt megvalósító DISSECT-CF-IoT, majd DISSECT-CF-Fog szimulátorokat Márkus Andrással, és kiértékeltek azokat különféle használati eseteket megvalósító scénáriókkal.

Az IoT-Köd-Felhő rendszerek területén végzett kutatásaink a DISSECT-CF-Fog szimulátor kifejlesztéséhez vezettek, mely a DISSECT-CF, föderált felhő infrastruktúrák vizsgálatát lehetővé tevő szimulátorra épül. Az alap szimulátor kiter-

jesztését négy területen végeztük el: IoT eszköz modellezés, felhő és IoT szolgáltatói árazás, kód és harmat (Dew Computing) infrastruktúra modellezés, valamint mobilitás, aktuáció és energia modellezés.

A felhő és IoT szolgáltatók árazási módszereinek vizsgálata alapján kidolgoztunk egy leírónyelvet [18], mellyel tetszőleges árazási modell kifejezhető, és a szimulátorba betöltve automatikus költségbecslés végezhető a szimulációs kísérletek lefuttatásával.

Az alap szimulátorban meglévő felhő erőforrások alkalmazására vonatkozó energiafogyasztási modellt kiterjesztettük IoT eszközök energiafogyasztási modelljével [33]. Ehhez irodalomkutatásban fellelhető fogyasztási adatokat és valós, szisztematikus méréseket is felhasználtunk kétféle mikrovezérlővel. Kiterjesztéseinkkel lehetővé vált több ezer IoT eszköz felhasználásával működő IoT alkalmazások szimulációja, az energiafogyasztás, infrastruktúra-bérlési költségbecslés és számítási erőforrás-használat figyelembevételével. A szimulátor komponenseinek implementációját Márkus András végezte.

3.3. Megterveztem egy metodológiát IoT-Köd-Felhő alkalmazások viselkedéselemzéséhez. A metodológia részeként kidolgoztunk különféle erőforrás-allokációs stratégiákat Márkus Andrással, melyek algoritmusai képesek csökkenteni az alkalmazások futási idejét és a felhasznált erőforrások költségét, egyúttal optimalizálva az IoT-Köd-Felhő infrastruktúra kihasználtságát. Az algoritmusokat kiértékeljük a DISSECT-CF-Fog szimulátorban, és bemutatjuk hatékonyságukat.

Kidolgoztunk egy feladat szétosztási (offloading) módszert Márkus Andrással a korábban megtervezett IoT és mobilitási modell DISSECT-CF-Fog-beli megvalósításának szemléltetéséhez, mely a számítási feladatok végrehajtásában részt vevő kód erőforrások túlterheltségét hivatott csökkenteni. A feladat szétosztási döntéseket az elérhető felhő és kód topológiák tulajdonságait figyelembe vevő, különféle alkalmazásvezérlési stratégiákat leíró algoritmusokkal valósítottuk meg. Az algoritmusok implementációját Márkus András végezte. Az allokációs stratégiákat részletesen kiértékeljük egy valós mérési adatokra épülő, európai szintű időjárás-előrejelző használati eset három scenáriójával [32]. A kiértékelés eredményei megmutatták a különféle stratégiák alkalmazásának előnyeit.

A mobilitási modell további bővítéseként kidolgoztunk egy aktuátor komponens a DISSECT-CF-Fog szimulátorhoz, mely képes a szimulált IoT eszközök viselkedését vagy környezetét befolyásolni. Ehhez kapcsolódóan kidolgoztuk az eszközök és számítási erőforrások (kód és felhő) GPS koordináták alapján történő földrajzi pozícióinak mentését ill. nyomon követését. Így lehetővé vált az IoT eszközök mozgásának valósághű modellezése, és mobilitást támogató erőforrásválasztó algoritmusok fejlesztése. Ezt követően különböző scenáriókkal (pl. logisztika) kiértékeljük a DISSECT-CF-Fog aktuációs és mobilitási kiterjesztéseit és a kapcsolódó

mozgási algoritmusokat (pl. véletlen bolyongás, nomád vándorlás) [16], melyekkel szemléltettük a kiterjesztések széles körű alkalmazhatóságát.

Karolj Skala (RBI, Zágráb, Horvátország) professzorral együttműködésben megvizsgáltuk, hogy az IoT eszközök erőforrásainak kihasználásával kialakítható hármat számítások (Dew Computing) hogyan modellezhetők a DISSECT-CF-Fog szimulátorban, és egy valós, drónokkal végzett időjárás monitorozó eset szimulációjával szemléltettük alkalmazását, melyhez egy Markov-modellre épülő szolgáltatás migráció előrejelző algoritmust fejlesztettünk [17].

Ebben a téziscsoportban felsorolt kutatási eredmények eléréséhez számos nemzetközi együttműködésben vettem részt, többek között a következő neves kutatóval: Karolj Skala (RBI, Zágráb, Horvátország). A 3. téziscsoporthoz tartozó publikációk: [15], [16], [17], [18], [26], [30], [32], [33].

## 4. téziscsoport: IoT-Blokklánc-Köd-Felhő rendszerek vizsgálata

4.1. Megterveztünk egy módszert kód és blokklánc rendszerek integrálására Baniata Hamzaval, és kidolgoztunk egy nyílt, bővíthető szimulátort vizsgálatukra, a FoBSim-et. A szimulátor alkalmazhatóságát számos blokklánc-telepítési scenárió elemzésével szemléltettük.

A Blokklánc technológia (BL, Blockchain) 2008-ban egy forradalmian új megközelítésként jelent meg az elosztott bizalom, decentralizált pénzügy és biztonság területén [42]. Ez a módszer egy megbízható, megmásíthatatlan és teljesen elosztott adatkezelést képes nyújtani az ún. elosztott főkönyvi technológia, mely megoldást jelenthet az IoT-Köd-Felhő rendszerek még megoldatlan bizalmi és biztonsági kihívásaira. Ezen rendszerek blokkláncokkal történő integrációját vizsgálva először egy részletes irodalomkutatást végeztünk [4], melyben áttekintettük a létező megoldásokat és jövőbeli megközelítéseket. Munkánk azt mutatta, hogy bár előnyös lehet a BL integráció, számos kihívás tapasztalható a standardizációs hiányosságokkal, magasabb késleltetéssel és energiafogyasztással, valamint a szociális bizalmatlansággal kapcsolatban.

Ezen kihívások egy részének megválaszolásához kidolgoztuk a FoBSim szimulációs környezetet [6], mely képes BL és kód integrációs lehetőségek elemzésére. A szimulátorban számos konszenzusos algoritmus (pl. PoW, PoS, PoA) hatékonyságát értékelhetjük ki, változatos blokklánc-telepítési paraméterek és igényelt kiszolgáló infrastruktúra megadásával. Az eszköz használatát számos scenárióval és vezérlő algoritmussal (pl. pletyka-alapú) szemléltettük. A szimulátor és a konszenzusos algoritmusok implementációját Baniata Hamza végezte.

- 4.2. Kidolgoztunk egy módszert Baniata Hamzaval a blokklánc hálózatok teljesítményének és konzisztenciájának elemzésére, melyet kiértékelünk a FoB-Sim eszközzel. Kidolgoztunk és kiértékelünk egy adattovábbítást optimalizáló protokollt, dinamikus szomszédválasztással teszi lehetővé a szomszédok számának minimalizálását.

A blokklánc-integráció optimalizációs lehetőségeinek feltárásához a BL rendszerekben tapasztalható forkolási jelenséget (forking phenomenon) vizsgáltuk meg egy valószínűségi végességi (probabilistic finality) módszerrel [31]. A PoW (Proof of Work) algoritmus viselkedését vizsgáltuk meg a FoBSim-ben számos konfigurációs paraméter szisztematikus változtatásával. Az elosztott főkönyv konzisztenciáját a rendszerben egy adott pillanatban jelen lévő forkok (azaz az egyes csomópontokon eltérő tartalommal rendelkező láncok) és a maximálisan előfordulható lánc verziók arányával definiáltuk. A kísérlet sorozatok lefuttatásával és kiértékelésével megmutattuk, hogy a bemeneti, környezeti paraméterek változtatása milyen hatással van a konzisztencia alakulására. Az eredmények igazolták, hogy a bányászok számának növelése csökkenti a konzisztencia szintet (és a forkok számát), de nem olyan hatékonyan, mintha a szomszédok számát növelnénk.

A BL hálózatokban alkalmazható pletyka-alapú információtovábbítás javítására kidolgoztunk egy dinamikus optimalizációs szomszédválasztó protokollt (DONS - Dynamic Optimized Neighbor Selection) [1]. A DONS protokoll alkalmazásával a hálózatban részt vevő bányászok szomszédainak számát minimalizálhatjuk azáltal, hogy egy minimális feszítő fát számolunk ki és alkalmazunk az adatok továbbításához. Megmutattuk, hogy a DONS módszer képes csökkenteni az adatgenerálástól az adat teljes hálózaton történő szétterítéséig eltelt időt. A kapcsolódó algoritmusok implementációját Baniata Hamza végezte.

A blokklánc rendszerek biztonságát illetően megvizsgáltuk, hogy a PoW algoritmust alkalmazó rendszerekben miként sérülhet a helyes működés biztosítása [5]. Nakamoto modelljét és a szakirodalomban fellelhető elméleti megközelítéseket elemezve (pl. AI-assisted mining, Quantum Computing, Sharding, Partial Pre-imagining), olyan gyakorlati módszereket fogalmaztunk meg, melyek alkalmazásával kisebbségi bányász birtoklás esetén is sérülhet a biztonság.

- 4.3. Megterveztem és kidolgoztam egy oltási információ validáló és nyomon követő módszert, mely köd- és felhő-alapú blokklánc rendszert alkalmaz. A módszer kiértékelését egy valós adatokkal dolgozó használati esettel végeztem el a FoBSim szimulátorral, különféle blokklánc-telepítési opciók elemzésével és összehasonlításával.

A COVID-19 pandémia 2020-as kitörését követően az egész világban elterjedt, és az okos rendszerek fejlődésére is hatással volt. A feltörekvő technológiák alkalmazása jelentős szerepet töltött be a vírus terjedésének korlátozásában, számos okos

alkalmazást fejlesztettek például az utazási korlátozások kezelésére és a társadalmi érintkezések csökkentésére. Hasonló céllal terveztem meg a VACFOB architektúrát (VACcination information validation and tracking with a FOg and cloud-based Blockchain system) [7], mely egy IoT-Blokklánc-Köd-Felhő rendszer alkalmazásával oltási információk magánszféra-védelmet biztosító nyomon követésére és ellenőrzésére használható. Három eltérő skálájú scenáriót definiáltam valós oltási jelentések számossága alapján, melyek adatkezelési követelményeiknek megfelelő teljesítményű blokklánc-telepítési eseteket vizsgáltam a FoBSim szimulátorral. Szisztematikus kísérletekkel határoztam meg a scenáriók egyes eseteit hatékonyan kiszolgáló blokklánc infrastruktúra méretét és alkalmazandó konszenzusos algoritmusait. Az eredmények hozzájárulhatnak a VACFOB módszer jövőbeli bevezetéséhez, és útmutatóként szolgálhatnak hasonló felépítésű és célú rendszerek tervezéséhez.

- 4.4. Kidolgoztunk egy metodológiát magánszféra-védelmet megvalósító kód-alapú blokklánc rendszerek tervezésére Baniata Hamzaval. Módszereit kiértékeljük egy kód és blokklánc infrastruktúrával támogatott felhős feladatütemezési alkalmazás szimulációjával, valamint egy valós intézmény akkreditációs és tanúsítvány validációs alkalmazással.

A blokklánc technológia megjelenése új lehetőségeket teremtett az erőforrás- és adatkezelés hatékonyságának növelésére IoT-Köd-Felhő rendszerekben. Baniata Hamza és Anaqreh Ahmad segítségével kidolgoztunk egy módszert (PF-BTS), mely hangya kolónia optimalizációs (ACO - Ant Colony Optimization) algoritmust alkalmaz egy kód és blokklánc infrastruktúrával támogatott feladatütemezés hatékony megvalósítására felhő rendszerekben [2]. A módszerben a blokkláncban részt vevő bányászok okos szerződések végrehajtásával generálnak különféle feladatallokációs terveket, melyek közül a leghatékonyabb terv kerül kiválasztásra. A PF-BTS módszert szimulációs környezetben értékeltük ki több feladatütemezési algoritmus összehasonlításával. Az algoritmusok és a szimulációs környezet implementációját Baniata Hamza végezte.

Napjaink online tanúsítványkezelő keretrendszereinek többsége nem rendelkezik megfelelő biztonsági és szolgáltatásminőségi garanciákkal. Ennek a problémának a megoldására dolgoztuk ki a PriFoB módszert a TruBlo EU H2020 projekt Fog-Block4Trust alprojektjében [3], mely kód- és blokklánc-alapú tanúsítványkezelést tesz lehetővé. Megoldásunkban egy nyilvános, engedélyköteles blokklánc rendszer kód infrastruktúrára működtetve, digitális aláírás és tudásmentes bizonyítás (Zero-Knowledge Proofs) módszereire építve egy GDPR-kompatibilis alkalmazást valósítottunk meg. Egyedi megközelítésünkben egymást kiegészítve alkalmazzuk a PoA (Proof of Authority) és a SoW (Signatures of Work) konszenzusos algoritmusokat tanúsítványkiállító intézmények akkreditációjára és ellenőrizhető tanú-

sítványok (Verifiable Credentials) biztonságos kezelésére. A tanúsítványokra vonatkozó adatokat egy körmentes gráf-alapú háromdimenziós főkönyvben (Three-Dimensional DAG-based Distributed Ledger - 3DDL) tároljuk, biztosítva a tanúsítványok visszavonásának lehetőségét. A javasolt megoldásunk teljesítményelemzésével megmutattuk hatékonyabb alkalmazhatóságát a jelentősebb blokklánc megoldásokkal összevetve (pl. Ethereum, Hyperledger Indy, Besu és Fabric), melyekkel szemben alacsonyabb írási és olvasási késleltetést tapasztaltunk, hasonló terheltség alatt. A PriFoB alkalmazás implementációját Baniata Hamza végezte.

Ebben a téziscsoportban felsorolt kutatási eredmények eléréséhez számos nemzetközi együttműködésben vettem részt, többek között a következő neves kutatóval: Radu Prodan (AAU, Klagenfurt, Ausztria). A 4. téziscsoporthoz tartozó publikációk: [1], [2], [3], [4], [5], [6], [7], [29], [31].

### 3. Az eredmények hasznosulása

Az értekezésben bemutatott kutatási eredmények nagy része az elnyert ösztöndíjaim (Magyary Zoltán Posztdoktori, Bolyai János Kutatási, és az Új Nemzeti Kiválóság Program Posztdoktori, valamint Fiatal oktatói, kutatói Ösztöndíjai), és az általam vezetett hazai OTKA FK-131793 projekt, és a nemzetközi TruBlo EU H2020 projekt szintén általam koordinált FogBlock4Trust alprojektjének sikeres megvalósítása során keletkeztek. Ezek mellett a hazai Élő Dolgok Internete (GINOP-2.3.2-15-2016-00037), a Smart Rendszerek Kutatóintézet (20391-3/2018/FEKUSTRAT, TUDFO/47138-1/2019-ITM és TKP2021-NVA-09) projektekben alprojektvezetéssel, valamint a hazai Mesterséges Intelligencia Nemzeti Laboratórium (MILAB), és a nemzetközi S-Cube EU FP7, ENTICE EU H2020, EU COST Action IC1304 (ACROSS), EU COST Action CA17136 (INDAIRPOLLNET), és EU COST Action CA19135 (CERCIRAS) projektekben való aktív részvételemmel is jelentős eredményeket értünk el.

Az itt bemutatott eredményeim közvetlen hatással voltak ezen projekteken kívüli, további kutatók munkájára is. Publikációim több, mint 1200 független hivatkozást generáltak, melyek közül számos cikk a kapcsolódó tématerületek vezető folyóirataiban és konferenciáin jelent meg. Az SLA-alapú felhős szolgáltatáskezeléshez kapcsolódó eredményeinket számos rangos fórumon hivatkozzák (pl. [38]), vonatkozó cikkeink a leghivatkozottabbak közé tartoznak ([10]-71 db és [14]-93 db). Az FCM megoldásunkat és a felhő-alapú rendszerekben történő adatkezelés jogi megfelelőségét elemző cikkünket a terület egyik leghivatkozottabb és legelismertebb kutatócsoportja, az ausztrál CLOUDS Lab is hivatkozta egy rangos folyóiratban [45]. Az IoT protokollok és brókerek összehasonlítását tárgyaló munkánk számos kutatás alapjául szolgál, jelenleg 106 hivatkozásnál jár.

A kidolgozott szimulátoraink potenciálisan alkalmazhatók, mind akadémiai algoritmus tervezésben, mind ipari rendszer- és alkalmazástervezési és elemzési folyamatokban. A MoBIoTSim félszimulációs megoldásunk elsőként tette lehetővé IoT környezetek szimulációját valós felhős szolgáltatásokkal kombinálva. Ezt a megoldást később több konkurens szimulátor fejlesztői hivatkozták (pl. FogNetSim++ [43]). A DISSECT-CF-Fog szimulátorban alkalmazott költségbecslési modellre több munkájában is hivatkozott a Pisai Egyetemen működő SOCC kutatócsoport, melyet kibővítve használtak fel megoldásaikban (pl. [36]). A FoBSim blokklánc szimulátorunkat a Stockholmi Egyetem kutatói használták fel szimulációk futtatásához személyazonosság-kezelő alkalmazások vizsgálatához [44].

Végezetül kutatói tevékenységem hatásaként számos bírálói tevékenységre kaptam felkérést: két rangos folyóiratban végzek szerkesztői munkát (Springer Grid Computing és Springer Cluster Computing); több, mint 35 folyóiratban végzek bírálói munkát; és több, mint 80 konferencián voltam programbizottsági tag.

## A Szerző hivatkozott publikációi

### Folyóiratcikkek

- [1] Hamza Baniata, Ahmad Anaqreh, and **Attila Kerteszh**. “DONS: Dynamic Optimized Neighbor Selection for smart blockchain networks”. In: *Future Generation Computer Systems* 130 (2022), pp. 75–90. DOI: 10.1016/j.future.2021.12.010.
- [2] Hamza Baniata, Ahmad Anaqreh, and **Attila Kerteszh**. “PF-BTS: A Privacy-Aware Fog-enhanced Blockchain-assisted task scheduling”. In: *Information Processing & Management* 58.1 (2021), p. 102393. DOI: 10.1016/j.ipm.2020.102393.
- [3] Hamza Baniata and **Attila Kerteszh**. “PriFoB: A Privacy-aware Fog-enhanced Blockchain-based system for Global Accreditation and Credential Verification”. In: *Journal of Network and Computer Applications* 205 (2022), p. 103440. DOI: 10.1016/j.jnca.2022.103440.
- [4] Hamza Baniata and **Attila Kerteszh**. “A Survey on Blockchain-Fog Integration Approaches”. In: *IEEE Access* 8 (2020), pp. 102657–102668. DOI: 10.1109/ACCESS.2020.2999213.
- [5] Hamza Baniata and **Attila Kerteszh**. “Approaches to Overpower Proof-of-Work Blockchains Despite Minority”. In: *IEEE Access* 11 (2023), pp. 2952–2967. DOI: 10.1109/ACCESS.2023.3234322.

- [6] Hamza Baniata and **Attila Kerteszesz**. “FoBSim: an extensible open-source simulation tool for integrated fog-blockchain systems”. In: *PeerJ Computer Science* 7 (2021), e431. DOI: doi.org/10.7717/peerj-cs.431.
- [7] **Attila Kerteszesz**. “Block the Chain: Software Weapons of Fighting Against COVID-19”. In: *Computer* 55.9 (2022), pp. 43–53. DOI: 10.1109/MC.2022.3147368.
- [8] **Attila Kerteszesz**. “Interoperable Data Management Using Personal and Infrastructure Clouds”. In: *IEEE Cloud Computing* 2.1 (2015), pp. 22–28. DOI: 10.1109/MCC.2015.9.
- [9] **Attila Kerteszesz**, Jozsef Daniel Dombi, and Attila Benyi. “A pliant-based virtual machine scheduling solution to improve the energy efficiency of iaas clouds”. In: *Journal of Grid Computing* 14 (2016), pp. 41–53. DOI: 10.1007/s10723-015-9336-9.
- [10] **Attila Kerteszesz**, Gabor Kecskemeti, and Ivona Brandic. “An interoperable and self-adaptive approach for SLA-based service virtualization in heterogeneous Cloud environments”. In: *Future Generation Computer Systems* 32 (2014), pp. 54–68. DOI: 10.1016/j.future.2012.05.016.
- [11] **Attila Kerteszesz**, Gabor Kecskemeti, Marc Oriol, Peter Kotcauer, Sandor Acs, Marc Rodriguez, Oscar Merce, Attila Marosi, Jordi Marco, and Xavier Franch. “Enhancing Federated Cloud Management with an Integrated Service Monitoring Approach”. In: *Journal of Grid Computing* 11.4 (2013), pp. 699–720. DOI: 10.1007/s10723-013-9269-0.
- [12] **Attila Kerteszesz**, Tamas Pflanzner, and Tibor Gyimothy. “A mobile IoT device simulator for IoT-Fog-Cloud systems”. In: *Journal of Grid Computing* 17.3 (2019), pp. 529–551. DOI: 10.1007/s10723-018-9468-9.
- [13] Dragi Kimovski, Attila Marosi, Sandi Gec, Nishant Saurabh, **Attila Kerteszesz**, Gabor Kecskemeti, Vlado Stankovski, and Radu Prodan. “Distributed environment for efficient virtual machine image management in federated Cloud architectures”. In: *Concurrency and Computation: Practice and Experience* 30.20 (2018), e4220. DOI: 10.1002/cpe.4220.
- [14] Kyriakos Kritikos, Barbara Pernici, Pierluigi Plebani, Cinzia Cappiello, Marco Comuzzi, Salima Benrernou, Ivona Brandic, **Attila Kerteszesz**, Michael Parkin, and Manuel Carro. “A Survey on Service Quality Description”. In: *ACM Comput. Surv.* 46.1 (2013). DOI: 10.1145/2522968.2522969.
- [15] Andras Markus and **Attila Kerteszesz**. “A survey and taxonomy of simulation environments modelling fog computing”. In: *Simulation Modelling Practice and Theory* 101 (2020). Modeling and Simulation of Fog Computing, p. 102042. DOI: 10.1016/j.simpat.2019.102042.



- [16] Andras Markus, Mate Biro, Gabor Kecskemeti, and **Attila Kerteszesz**. “Actuator behaviour modelling in IoT-Fog-Cloud simulation”. In: *PeerJ Computer Science* 7 (July 2021), e651. DOI: 10.7717/peerj-cs.651.
- [17] Andras Markus, Mate Biro, Karolj Skala, Zorislav Sojat, and **Attila Kerteszesz**. “Modeling Dew Computing in DISSECT-CF-Fog”. In: *Applied Sciences* 12.17 (2022). DOI: 10.3390/app12178809.
- [18] Andras Markus, **Attila Kerteszesz**, and Gabor Kecskemeti. “Cost-aware iot extension of dissect-cf”. In: *Future Internet* 9.3 (2017), p. 47. DOI: 10.3390/fi9030047.
- [19] Biswajeeban Mishra and **Attila Kerteszesz**. “The Use of MQTT in M2M and IoT Systems: A Survey”. In: *IEEE Access* 8 (2020), pp. 201071–201086. DOI: 10.1109/ACCESS.2020.3035849.
- [20] Biswajeeban Mishra, Biswaranjan Mishra, and **Attila Kerteszesz**. “Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements”. In: *Energies* 14.18 (2021). DOI: 10.3390/en14185817.
- [21] Tamas Pflanzner and **Attila Kerteszesz**. “A Taxonomy and Survey of IoT Cloud Applications”. In: *EAI Endorsed Transactions on Internet of Things* 3.12 (Oct. 2017). DOI: 10.4108/eai.6-4-2018.154391.
- [22] Szilvia Varadi, **Attila Kerteszesz**, and Michael Parkin. “The necessity of legally compliant data management in European cloud architectures”. In: *Computer Law Security Review* 28.5 (2012), pp. 577–586. DOI: 10.1016/j.clsr.2012.05.006.

## Könyvfejezetek

- [23] Wojciech Burakowski, Andrzej Beben, Hans van den Berg, Joost W Bosman, Gerhard Hasslinger, **Attila Kerteszesz**, Steven Latre, Rob van der Mei, Tamas Pflanzner, Patrick Gwydion Poullie, et al. “Traffic management for cloud federation”. In: *Autonomous Control for a Reliable Internet of Services*. Springer, Cham, 2018, pp. 269–312. DOI: 10.1007/978-3-319-90415-3\_11.
- [24] **Attila Kerteszesz**. “Characterizing Cloud Federation Approaches”. In: *Cloud Computing: Challenges, Limitations and R&D Solutions*. Ed. by Zaigham Mahmood. Cham: Springer International Publishing, 2014, pp. 277–296. DOI: 10.1007/978-3-319-10530-7\_12.
- [25] **Attila Kerteszesz** and Szilvia Varadi. “Legal Aspects of Data Protection in Cloud Federations”. In: *Security, Privacy and Trust in Cloud Systems*. Ed. by Surya Nepal and Mukaddim Pathan. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 433–455. DOI: 10.1007/978-3-642-38586-5\_15.

- [26] Andras Markus and **Attila Kerteszesz**. “Investigating IoT Application Behaviour in Simulated Fog Environments”. In: *Cloud Computing and Services Science*. Ed. by Donald Ferguson, Claus Pahl, and Markus Helfert. Cham: Springer International Publishing, 2021, pp. 258–276. DOI: 10.1007/978-3-030-72369-9\_11.
- [27] Tamas Pflanzner, Miklos Hovari, Imre Vass, and **Attila Kerteszesz**. “Designing an IoT-Cloud Gateway for the Internet of Living Things”. In: *International Conference on Cloud Computing and Services Science*. Springer. 2019, pp. 23–41. DOI: 10.1007/978-3-030-49432-2\_2.
- [28] Szilvia Varadi, Gizem Gultekin Varkonyi, and **Attila Kerteszesz**. “Legal Issues of Social IoT Services: The Effects of Using Clouds, Fogs and AI”. In: *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications: Emerging Technologies for Connected and Smart Social Objects*. Ed. by Aboul Ella Hassanien, Roheet Bhatnagar, Nour Eldeen M. Khalifa, and Mohamed Hamed N. Taha. Cham: Springer International Publishing, 2020, pp. 123–138. DOI: 10.1007/978-3-030-24513-9\_7.

## Konferenciatickek

- [29] Hamza Baniata, Dragi Kimovski, Radu Prodan, and **Attila Kerteszesz**. “Towards Blockchain-based Smart Systems”. In: *CEUR Workshop Proceedings*. Vol. 3145. 2021.
- [30] Edua Eszter Kalmar and **Attila Kerteszesz**. “What Does I(o)T Cost?” In: *Proceedings of the 8th ACM/SPEC on International Conference on Performance Engineering Companion*. ICPE ’17 Companion. L’Aquila, Italy: Association for Computing Machinery, 2017, pp. 19–24. DOI: 10.1145/3053600.3053601.
- [31] **Attila Kerteszesz** and Hamza Baniata. “Consistency Analysis of Distributed Ledgers in Fog-Enhanced Blockchains”. In: *Euro-Par 2021: Parallel Processing Workshops*. Ed. by Ricardo Chaves et al. Cham: Springer International Publishing, 2022, pp. 393–404. DOI: 10.1007/978-3-031-06156-1\_31.
- [32] Andras Markus, Jozsef Daniel Dombi, and **Attila Kerteszesz**. “Location-aware Task Allocation Strategies for IoT-Fog-Cloud Environments”. In: *2021 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)*. 2021, pp. 185–192. DOI: 10.1109/PDP52278.2021.00037.

- [33] Andras Markus and **Attila Kerteszes**. “Modelling Energy Consumption of IoT Devices in DISSECT-CF-Fog”. In: *Proceedings of the 11th International Conference on Cloud Computing and Services Science*. SCITEPRESS - Science and Technology Publications, 2021. DOI: 10.5220/0010500003200327.
- [34] Tamas Pflanzner, Zoltan Feher, and **Attila Kerteszes**. “A Crawling Approach to Facilitate Open IoT Data Archiving and Reuse”. In: *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. IEEE. 2019, pp. 235–242. DOI: 10.1109/IOTSMS48152.2019.8939248.
- [35] Tamas Pflanzner and **Attila Kerteszes**. “A Private Gateway for Investigating IoT Data Management”. In: *Proceedings of the 8th International Conference on Cloud Computing and Services Science, CLOSER 2018, Funchal, Madeira, Portugal, March 19-21, 2018*. Ed. by Victor Méndez Muñoz, Donald Ferguson, Markus Helfert, and Claus Pahl. SciTePress, 2018, pp. 526–532. DOI: 10.5220/0006775505260532.

## További hivatkozott közlemények

- [36] Antonio Brogi, Stefano Forti, and Ahmad Ibrahim. “Optimising QoS-Assurance, Resource Usage and Cost of Fog Application Deployments”. In: *Cloud Computing and Services Science*. Ed. by Victor Mendez Munoz, Donald Ferguson, Markus Helfert, and Claus Pahl. Cham: Springer International Publishing, 2019, pp. 168–189. DOI: 10.1007/978-3-030-29193-8\_9.
- [37] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility”. In: *Future Generation Computer Systems* 25.6 (2009), pp. 599–616. DOI: 10.1016/j.future.2008.12.001.
- [38] Florian Daniel, Pavel Kucherbaev, Cinzia Cappiello, Boualem Benatallah, and Mohammad Allahbakhsh. “Quality Control in Crowdsourcing: A Survey of Quality Attributes, Assessment Techniques, and Assurance Actions”. In: *ACM Comput. Surv.* 51.1 (Jan. 2018). DOI: 10.1145/3148148.
- [39] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. “Internet of Things (IoT): A vision, architectural elements, and future directions”. In: *Future generation computer systems* 29.7 (2013), pp. 1645–1660. DOI: 10.1016/j.future.2013.01.010.

- [40] Redowan Mahmud, Ramamohanarao Kotagiri, and Rajkumar Buyya. “Fog Computing: A Taxonomy, Survey and Future Directions”. In: *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives* (2018), pp. 103–130. DOI: 10.1007/978-981-10-5861-5\_5.
- [41] Redowan Mahmud, Ramamohanarao Kotagiri, and Rajkumar Buyya. “Fog Computing: A Taxonomy, Survey and Future Directions”. In: *Internet of Everything: Algorithms, Methodologies, Technologies and Perspectives*. Ed. by Beniamino Di Martino, Kuan-Ching Li, Laurence T. Yang, and Antonio Esposito. Singapore: Springer Singapore, 2018, pp. 103–130. DOI: 10.1007/978-981-10-5861-5\_5.
- [42] Satoshi Nakamoto. “Bitcoin: A peer-to-peer electronic cash system”. In: *Decentralized business review* (2008), p. 21260.
- [43] Tariq Qayyum, Asad Waqar Malik, Muazzam A. Khan Khattak, Osman Khalid, and Samee U. Khan. “FogNetSim++: A Toolkit for Modeling and Simulation of Distributed Fog Environment”. In: *IEEE Access* 6 (2018), pp. 63570–63583. DOI: 10.1109/ACCESS.2018.2877696.
- [44] Kazi Masum Sadique, Rahim Rahmani, and Paul Johannesson. “DIdM-ElIoT: Distributed Identity Management for Edge Internet of Things (IoT) Devices”. In: *Sensors* 23.8 (2023). DOI: 10.3390/s23084046.
- [45] Adel Nadjaran Toosi, Rodrigo N. Calheiros, and Rajkumar Buyya. “Inter-connected Cloud Computing Environments: Challenges, Taxonomy, and Survey”. In: *ACM Comput. Surv.* 47.1 (May 2014). DOI: 10.1145/2593512.