International Journal of Engineering and Management Sciences (IJEMS) (2025) **Online First**
*DOI: 10.21791/IJEMS.2025.03.*

*Review paper*

# Kiberbiztonsági kihívások a mezőgazdaság digitalizációjában: Szisztematikus áttekintés Python-alapú elemzéssel

# Cybersecurity Challenges in Agricultural Digitalization: A Systematic Review with Python-Based Analysis

PORKOLÁB-ANGYALOS ZSANETT[1]

[1]Debreceni Egyetem, Gazdaságtudományi Kar, Gazdálkodás- és Szervezéstudományok Doktori Iskola, Debrecen. Magyarország. angyalos@mailbox.unideb.hu

*Abstract. A mezőgazdaság és a kiberbiztonság metszéspontja az IoT (Internet of Things) és a precíziós gazdálkodás gyors térnyerése révén az utóbbi években a kutatás egyik kiemelt területévé vált. Ezek a technológiai innovációk forradalmasították a mezőgazdasági folyamatokat, javítva a hatékonyságot és a fenntarthatóságot, ugyanakkor jelentős biztonsági kockázatokat is hoztak magukkal. Ez a tanulmány szisztematikus irodalomkutatást (Systemeatic Literature Review - SLR) végez a mezőgazdaság kiberbiztonságának kulcskérdéseiről, különös tekintettel az IoT sebezhetőségeire és a fenyegetésekre. A kutatás során Python-alapú szövegelemzési technikák segítségével automatizáltam az absztraktok és teljes szövegek elemzését, lehetővé téve a releváns tanulmányok gyors szűrését és tematikus csoportosítását. Az elemzett 1039 publikáció közül szigorú szűrési kritériumok alapján 40 releváns tanulmányt azonosítottam. A tematikus elemzés eredménye szerint a publikációk 44,9%-a az IoT eszközök sebezhetőségeire, 32,7%-a a mezőgazdasági kiberbiztonsági kihívásokra, míg 22,4%-a az Agriculture 4.0 és precíziós gazdálkodás biztonsági kérdéseire összpontosított. A módszertani megoszlás vizsgálata során kiderült, hogy a kutatásokban a gépi tanulás, a szimulációs modellek és az esettanulmányok dominálnak, míg a felmérések és a kísérleti kutatások kisebb arányban fordulnak elő. Az eredmények rávilágítanak arra, hogy a mezőgazdasági szektorban alapvető fontosságú a kiberbiztonsági stratégiák és technológiák fejlesztése, különösen az IoT eszközök által hordozott kockázatok csökkentése érdekében.*

*Kulcsszavak: kiberbiztonság, mezőgazdaság, Python, SLM*

*Abstract. The intersection of agriculture and cybersecurity has become a prominent research focus in recent years, driven by the rapid adoption of IoT (Internet of Things) and precision farming technologies. These technological innovations have revolutionized agricultural processes, enhancing efficiency and sustainability while introducing significant security risks. This study conducts a systematic literature review (SLR) to address key cybersecurity issues in agriculture, with a particular emphasis on IoT vulnerabilities and threats. Using Python-based text analysis techniques, the research automated the analysis of abstracts and full texts, enabling rapid filtering and thematic categorization of relevant studies. From an initial pool of 1,039 publications, 40 relevant studies were identified based on rigorous screening criteria. The thematic analysis revealed that 44.9% of the publications focus on IoT device vulnerabilities, 32.7% on agricultural cybersecurity challenges, and 22.4% on the security issues of Agriculture 4.0*

*DOI: 10.21791/IJEMS.2025.03.*

*and precision farming. Methodological analysis indicated that machine learning, simulation models, and case studies dominate the research landscape, while surveys and experimental studies appear less frequently. The findings highlight the critical importance of developing robust cybersecurity strategies and technologies in the agricultural sector, particularly to mitigate the risks posed by IoT devices.*

*Keywords: Cybersecurity, Agriculture, Python, SLM*

# Bevezetés

A mezőgazdaság az emberiség egyik legfontosabb gazdasági és társadalmi ágazata, amely az elmúlt évtizedekben a technológiai innovációknak köszönhetően jelentős átalakuláson ment keresztül. Az olyan digitális eszközök, mint az IoT (Internet of Things) technológiák és a precíziós gazdálkodás, forradalmasították a termelési folyamatokat, lehetővé téve a hatékonyabb munkavégzést, a környezeti terhelés csökkentését és a termelékenység növelését.

Az Internet of Things (IoT) kulcsfontosságú szerepet játszik a modern mezőgazdaság fejlődésében. Az IoT eszközök hálózata valós időben gyűjt és oszt meg adatokat, amely alapvető betekintést nyújt a gazdálkodóknak a termelési környezetükbe [15]. Például az IoT-alapú talajnedvesség-érzékelők lehetővé teszik az öntözés pontos időzítését, ezzel vizet takarítva meg és javítva a növények egészségét. Hasonlóképpen, az IoT-val támogatott állattartási rendszerek figyelemmel kísérhetik az állatok egészségi állapotát és viselkedését, elősegítve az időben történő beavatkozásokat és növelve a termelékenységet [1]. Ugyanakkor ezek az innovációk új típusú fenyegetéseket is hoztak magukkal, amelyek közül kiemelkednek a kiberbiztonsági kockázatok. [8]

A különböző gyártók által kifejlesztett IoT-eszközök más és más biztonsági protokollokat alkalmaznak, ami egyenetlenségeket okoz az eszközök biztonságában és integrációjában [4].

További kritikus probléma a gyenge hitelesítési rendszerek használata. Az alapértelmezett vagy könnyen kitalálható jelszavak, illetve a többfaktoros hitelesítés (MFA) hiánya jelentősen növeli az eszközök sebezhetőségét. Ezek a biztonsági hiányosságok lehetővé teszik a támadók számára, hogy átvegyék az irányítást az eszközök felett, adatokat szerezzenek meg, vagy akadályozzák a gazdaság működését [2]. Egy ilyen támadás során például az öntözőrendszereket manipulálhatják, vagy az állatállományt figyelő eszközök működését zavarhatják meg, amely jelentős veszteségeket eredményezhet a gazdálkodók számára. [8]

Ahogy az intelligens farmok egyre inkább támaszkodnak az összekapcsolt technológiákra, úgy válik a kiberbiztonság kiemelkedően fontossá a működésük szempontjából [8]. Az automatizáció és a robotika forradalmasítja az intelligens mezőgazdaságot azáltal, hogy precízen és hatékonyan látja el a monoton és munkaigényes feladatokat. Az olyan gépek, mint a drónok, automatizált traktorok és betakarítógépek, képesek önállóan elvégezni az ültetést, permetezést, gyomirtást és betakarítást, ezzel jelentősen csökkentve az emberi beavatkozás szükségességét. Az állattenyésztésben is terjednek az automatizált megoldások, például az automata etető- és fejőberendezések, amelyek nemcsak hatékonyabbá teszik a gazdálkodást, hanem hozzájárulnak az állatok jobb gondozásához és jólétéhez [5].

Az utóbbi években a mezőgazdasági technológiák és a kiberbiztonság metszetével foglalkozó tudományos publikációk száma drámai növekedést mutatott, ami rávilágít a téma fontosságára. Az

*DOI: 10.21791/IJEMS.2025.03.*

alábbi grafikon szemlélteti a megjelent szakirodalmi anyagok számának növekedését 2004-től napjainkig. A 2017-et követő években tapasztalható ugrás különösen a mezőgazdasági IoT-eszközök gyors térnyerésével magyarázható, amely új kiberbiztonsági kihívásokkal szembesíti az ágazat szereplőit.


*1.ábra: Évenként megjelent a témával kapcsolatos szakirodalmak száma*
*(Forrás: Saját készítés)*

A precíziós gazdálkodási rendszerek működése nagymértékben adatalapú, ami különösen érzékennyé teszi őket az adatmanipulációra és a kibertámadásokra. Ezek a támadások nemcsak működési zavarokat, hanem jelentős gazdasági veszteségeket is okozhatnak az agrárszektor szereplői számára [10]. Az ENSZ előrejelzései szerint a világ népessége 2050-re eléri a 9,8 milliárdot, ami az élelmiszertermelés jelentős növelését teszi szükségessé. Az innovációs technológiák kulcsszerepet játszanak a termelékenység növelésében, ugyanakkor jelentős kiberbiztonsági kihívásokat is jelentenek az agrár- és élelmiszeripar számára [14].

A modern mezőgazdasági rendszerek biztonságos és fenntartható működéséhez elengedhetetlen a digitális eszközök és hálózatok megfelelő védelme. Az adatintegritás és a rendszerek ellenállóképességének biztosítása kulcsfontosságú ahhoz, hogy ezek a technológiák hozzájáruljanak a fenntartható élelmiszertermeléshez és az agrárszektor hosszú távú fejlődéséhez [11].

Kutatási kérdések és célok

A kutatás során az alábbi kérdésekre kerestem választ:

1. Hogyan hat az IoT-eszközök mezőgazdasági alkalmazása a kiberbiztonsági kihívásokra?
2. Milyen típusú kiberfenyegetések érintik a leginkább a mezőgazdaságot?

*DOI: 10.21791/IJEMS.2025.03.*

# 1. Anyag és módszer

A tanulmány a szisztematikus irodalomkutatás (Systematic Literature Review, SLR) módszertanát alkalmazza, amely a PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) irányelveken alapul. [7] Ez a módszer lehetővé teszi az adott kutatási terület legfontosabb eredményeinek azonosítását, összegzését és kritikai értékelését, hogy átfogó képet nyújtson a mezőgazdaság digitalizációjának és kiberbiztonsági kihívásainak kapcsolódásáról.
A módszertan első lépéseként a kutatási kérdések meghatározására került sor (lásd: Bevezetés). A dokumentum későbbi fejezeteiben kerülnek bemutatásra az elemzéshez használt elektronikus adatbázisok, a keresési kifejezések, valamint a tanulmányok kiválasztásához alkalmazott kritériumok.

## 1.1. Adatforrások és keresési stratégia

Az irodalomkutatás során három tudományos adatbázist használtam: Web of Science, Dimensions AI és IEEE Xplore Digital Library. Ezek az adatbázisok széles körű hozzáférést biztosítanak a releváns tudományos cikkekhez, konferenciaanyagokhoz és más szakirodalmi forrásokhoz.

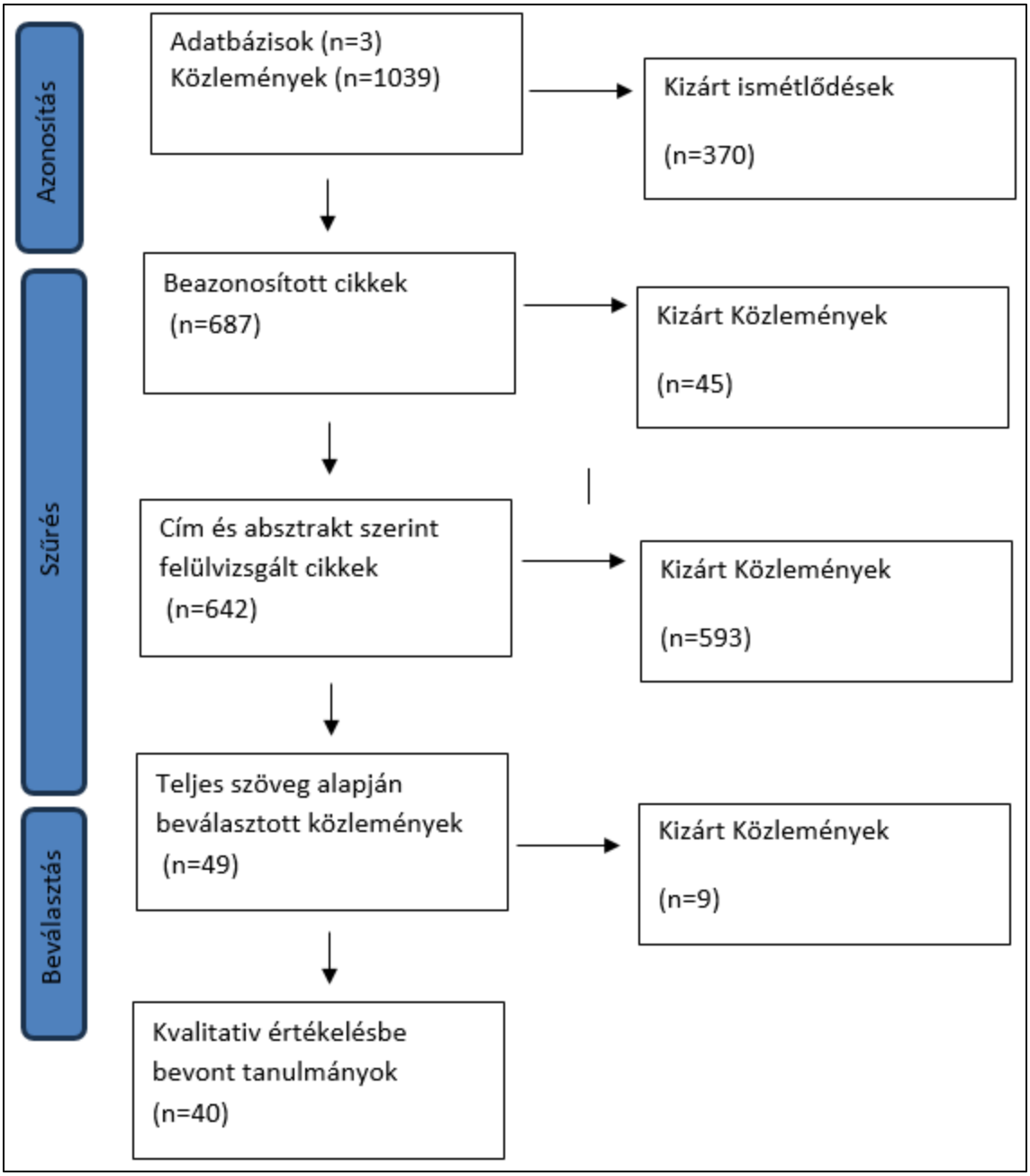
A keresési stratégia a következő kulcsszavakon és azok logikai kombinációin alapult:
cybersecurity, agriculture, smart farming, cyber attack, precision agriculture, cyber threats, IoT, data security
A szisztematikus irodalmi áttekintés folyamatábráját az 2. számú ábra mutatja be.

## 1.2. Alkalmassági kritériumok

A szűrési folyamat két lépésben zajlott: először a tanulmányok címét és absztraktját értékeltem, majd a relevánsnak ítélt találatok teljes szövegét vizsgáltam meg. Az alábbi kritériumok alapján döntöttem a tanulmányok alkalmasságáról:

- Hozzáférhetőség: Csak olyan irodalmakat vettem figyelembe, amelyek nyilvánosan elérhetők voltak, vagy amelyekhez a rendelkezésemre álló források (pl. egyetemi könyvtárak) révén hozzáfértem.
- Nyelvi korlátozás: A kutatásba kizárólag angol nyelvű tanulmányokat vontam be, mivel ezek biztosítják a legnagyobb lefedettséget a nemzetközi szakirodalomban.
- Tartalmi fókusz: Bár számos kiberbiztonsági tanulmány említi a mezőgazdaságot, csak azokat vettem be az elemzésbe, amelyek kifejezetten a mezőgazdaság biztonságával foglalkoznak.

*DOI: 10.21791/IJEMS.2025.03.*




*2.ábra: A szakirodalom kiválasztásának folyamatábrája a PRISMA modell alapján.*
*(Forrás: Saját készítés)*

## 1.3. Adatgyűjtés

A kutatás során az összes releváns tanulmányt Research Information Systems (RIS) formátumban exportáltam a Dimensions AI, Web of Science és IEEE Xplore Digital adatbázisokból. Az exportált fájlokat a szisztematikus irodalomkutatásra specializált Rayyan platformra importáltam, ahol az elsődleges szűrés zajlott (duplikációk kizárása). Az absztraktok és címek, valamint később a teljes szöveg értékelését Python segítségével végeztem.

A Python alkalmazása az automatizált elemzések során nemcsak az irodalomkutatás hatékonyságát növelte, hanem hozzájárult a tartalmi és módszertani összefüggések részletesebb feltárásához is.

*DOI: 10.21791/IJEMS.2025.03.*

Az absztrakt- és címszűrés eredményeiről, valamint az elutasított és bevont tanulmányok számáról a kutatás eredményei szakaszban adok részletes áttekintést.

## 1.4. Szűrés folyamata

A kutatás során átfogó és szisztematikus irodalomkutatást végeztem a Web of Science, Dimensions AI és IEEE Xplore Digital Library adatbázisok felhasználásával. Az összegyűjtött 1039 publikációból az ismétlődő tételek kiszűrését követően 687 egyedi szakirodalmi forrás maradt, amelyeket szövegbányászati technikák segítségével vizsgáltam.
Az elemzési folyamat során a TF-IDF (Term Frequency-Inverse Document Frequency) és a koszinusz-hasonlóság módszereit alkalmaztam a publikációk relevanciájának és tematikus összefüggéseinek feltárására. Ezek a technikák lehetővé tették a mezőgazdasági és kiberbiztonsági témákhoz kapcsolódó kulcsszavak kvantitatív elemzését és a tanulmányok pontos kategorizálását.

TF-IDF (Term Frequency-Inverse Document Frequency)
A TF-IDF (Term Frequency-Inverse Document Frequency) egy jól ismert szövegelemzési technika, amely egy adott szó fontosságát méri egy dokumentumban viszonyítva annak gyakoriságához egy teljes dokumentumgyűjteményben. A módszer két fő komponensből áll:

- Term Frequency (TF): A szó előfordulási gyakorisága egy adott dokumentumban, amely az adott szó jelentőségét méri az adott szövegen belül.
- Inverse Document Frequency (IDF): Az adott szó ritkasága az egész korpuszban, amely az általános használatból fakadó redundanciát csökkenti.

A TF-IDF modell hatékonyan alkalmazható nagy szöveges korpuszokban a releváns kulcsszavak azonosítására, amelyek jellemzőek egy adott dokumentumra, de kevésbé gyakoriak a teljes adatállományban. A mezőgazdasági biztonság tanulmányozása során a TF-IDF segített a releváns mezőgazdasági és kiberbiztonsági kulcsszavak azonosításában, lehetővé téve a szakirodalom relevanciájának kvantitatív értékelését. A módszer különösen jól használható strukturált és szabványosított szöveges korpuszok elemzésére, ahol a dokumentumok közötti különbségek jól körülhatárolhatók. [9]

Koszinusz-hasonlóság az adatelemzésben
A koszinusz-hasonlóság egy olyan mérőszám, amely a szöveges adatok tartalmi hasonlóságát méri vektoralapú megközelítéssel. Ez a módszer a dokumentumok szavainak gyakoriságát vektorként kezeli, és az általuk bezárt szög koszinuszát számítja ki. Az érték 0 és 1 között mozog, ahol az 1 teljes egyezést jelent.
Ez a technika különösen hasznos szövegek automatikus összehasonlítására, például dokumentumok tematikus csoportosítására vagy hasonlóság alapú osztályozásra. A kutatásomban a koszinusz-hasonlóságot alkalmaztam az "ismeretlen" kategóriába tartozó absztraktok legközelebbi tematikus csoporthoz rendelésére, így pontosabb és gyorsabb elemzést értem el. Erről az eredményekben lesz részletes információ.

A 687 szakirodalmi forrást Python alapú szövegelemzési technikák alkalmazásával tematikus szempontok szerint csoportosítottam. A tematikus csoportosítás célja az volt, hogy átfogó és

*DOI: 10.21791/IJEMS.2025.03.*

rendszerezett képet kapjak a mezőgazdasági kiberbiztonság területén végzett kutatásokról, feltárva az ágazatot érintő legfontosabb kihívásokat és trendeket. Az elemzés során az alábbi hét tematikus kategóriát határoztam meg:

Kiberbiztonsági kihívások a mezőgazdaságban
Ebbe a csoportba azok a tanulmányok tartoznak, amelyek a mezőgazdasági ágazatot érintő támadásokkal, például rosszindulatú programokkal, ransomware támadásokkal, DDoS támadásokkal és egyéb fenyegetésekkel foglalkoznak. A tanulmányok fókuszában a fenyegetések azonosítása és hatásainak vizsgálata áll.
Az alábbi kulcsszavakat határoztam meg: cyber threats, malware, ransomware, DDoS, cyberattack.

IoT és okos eszközök sebezhetősége
Az IoT-eszközök és okos mezőgazdasági eszközök sebezhetőségeit vizsgáló tanulmányok kaptak helyet ebben a csoportban. A kutatások elemzik az IoT-eszközök, szenzorhálózatok és egyéb okos megoldások biztonsági réseit és az ezekből adódó fenyegetéseket.
Kulcsszavak: IoT, Internet of Things, smart devices, sensor networks.

Agriculture 4.0 és precíziós gazdálkodás
Ez a csoport az Agriculture 4.0 és a precíziós gazdálkodási rendszerek biztonsági aspektusait tárgyalja. A kutatások középpontjában az automatizáció, a drónok használata és az adatvezérelt mezőgazdasági megoldások kiberbiztonsági kérdései állnak.
Kulcsszavak: precision agriculture, smart farming, automation, drones.

Adatbiztonság és adatvédelem a mezőgazdaságban
Az ebbe a csoportba tartozó tanulmányok a mezőgazdasági rendszerek adatbiztonságával és adatvédelmével foglalkoznak.
Kulcsszavak: data security, privacy, data integrity, data breach.

Kiberbiztonsági megoldások és stratégiák
E kategóriába kerültek azok a tanulmányok, amelyek konkrét kiberbiztonsági megoldásokat és stratégiákat mutatnak be, például titkosítási módszereket, tűzfalakat, behatolásészlelő rendszereket és egyéb védelmi technológiákat.
Kulcsszavak: cybersecurity solutions, encryption, firewalls, intrusion detection.

Blockchain technológia a mezőgazdaságban
A blockchain technológia mezőgazdasági alkalmazásaival foglalkozó tanulmányok alkotják ezt a csoportot. A kutatások a blokklánc technológia használatának előnyeit vizsgálják az ellátási lánc biztonsága és az élelmiszerek nyomon követhetősége terén.
Kulcsszavak: blockchain, traceability, supply chain security

Kiberbiztonság a fenntartható mezőgazdaságban

*DOI: 10.21791/IJEMS.2025.03.*

Ez a csoport a fenntartható mezőgazdaság és a kiberbiztonság kapcsolatát elemzi. A kutatások a zöld technológiák, a környezeti védelem és az erőforrás-hatékonyság biztonsági aspektusaira összpontosítanak.
Kulcsszavak: sustainability, green farming, environmental protection.

# 2. Eredmények és azok értékelése

A mezőgazdasági kiberbiztonsági szakirodalom tematikus elemzéséhez különböző Python-alapú szövegbányászati és adatelemzési technikákat alkalmaztam, amelyek lehetővé tették a szakirodalmi források hatékony kategorizálását és tartalmi összefüggéseik feltárását. Az elemzés során a pandas könyvtárat használtam az absztraktok adatainak betöltésére és előfeldolgozására, amely lehetővé tette az adatok strukturált kezelését és az egyes absztraktok feldolgozását. Az absztraktok kategorizálására a szövegek előforduló kulcsszavak alapján történő besorolására egyedi függvényt hoztam létre, amely az adott kulcsszavakat tartalmazó absztraktokat a megfelelő tematikus csoportba rendelte.
Az automatizált kategorizálás továbbfejlesztése érdekében az sklearn.feature_extraction.text modulból a TfidfVectorizer függvényt alkalmaztam, amely lehetővé tette a szakirodalmi források kulcsszó-alapú súlyozását és fontosságának meghatározását. A releváns kategóriák azonosításához és az "ismeretlen" kategóriába sorolt absztraktok besorolásához a sklearn.metrics.pairwise modulból a cosine_similarity függvényt használtam, amely a szövegek közötti tartalmi hasonlóság mérésére szolgált. Az így nyert eredmények segítettek abban, hogy a kezdetben nem egyértelműen besorolt absztraktokat a legrelevánsabb kategóriába rendezzem.

A csoportosítás eredménye a következő ábrán látható.

| | Kategória | Szakirodalmak száma ▾ |
|---|---|---|
| 1. | IoT és okos eszközök sebezhetősége | 383 |
| 2. | Kiberbiztonsági kihivások a mezőgazdaságban | 165 |
| 3. | Agriculture 4.0 és precíziós gazdálkodás | 62 |
| 4. | Adatbiztonság és adatvédelem a mezőgazdaságban | 32 |
| 5. | Blockchain technológia a mezőgazdaságban | 24 |
| 6. | Kiberbiztonsági megoldások es stratégiák | 12 |
| 7. | Kiberbiztonság a fenntartható mezőgazdaságban | 9 |
| | **Grand total** | **687** |
| | | 1 - 7 / 7 < > |

*3.ábra: Tematikus besorolás*
*Forrás: Saját készítés*

A csoportosítás eredményeként a legnagyobb arányban az IoT és okos eszközök sebezhetősége témakör szerepelt, amely 383 tanulmányban került elemzésre. Ez rámutat arra, hogy az IoT-eszközök széles körű elterjedése a mezőgazdaságban komoly biztonsági kihívásokat jelent, amelyeket megfelelő védelmi intézkedésekkel kell kezelni. [13]

*DOI: 10.21791/IJEMS.2025.03.*

A kiberbiztonsági kihívások a mezőgazdaságban kategóriában 165 tanulmányt azonosítottam, amelyek olyan fenyegetéseket vizsgálnak, mint a rosszindulatú szoftverek, zsarolóvírusok és szolgáltatásmegtagadási (DDoS) támadások. Az eredmények alapján megállapítható, hogy a mezőgazdasági vállalkozások számára különösen fontos az IT-biztonság megerősítése, hiszen a digitális rendszerek védelme kulcsfontosságú a működés fenntarthatósága szempontjából.

Az Agriculture 4.0 és precíziós gazdálkodás témaköre 62 tanulmányban jelent meg, amelyek arra világítanak rá, hogy a modern digitális technológiák egyre szélesebb körű alkalmazása új biztonsági kihívásokat eredményez az agrárszektor számára. A precíziós gazdálkodás során keletkező érzékeny adatok megfelelő védelme elengedhetetlen a hatékony és biztonságos működés érdekében. [6]

Az adatbiztonság és adatvédelem témakör 32 tanulmányban szerepelt, kiemelve az érzékeny információk védelmének fontosságát a mezőgazdasági vállalatok körében. Az adatvédelmi szabályozásoknak való megfelelés és a személyes adatok biztonsága kiemelt jelentőségű az ágazat számára.

A kisebb kategóriák, mint a blockchain technológia (24 tanulmány), a kiberbiztonság a fenntartható mezőgazdaságban (9 tanulmány), és a kiberbiztonsági megoldások és stratégiák (12 tanulmány), szűkebb fókuszúak, és kevésbé kapcsolódnak szorosan a kutatás központi kérdéseihez.

Ezért a kutatási fókusz szűkítése érdekében az IoT és okos eszközök sebezhetősége, a kiberbiztonsági kihívások, az Agriculture 4.0 és precíziós gazdálkodás, valamint az adatbiztonság és adatvédelem kategóriák kerültek megtartásra, a fennmaradó három kategóriát kizártam, mivel azok kevésbé voltak relevánsak a kutatás fókuszára nézve, így a további vizsgálathoz 642 szakirodalmi tételt tartottam meg.

A szakirodalmak számának további csökkentése érdekében egy TF-IDF (Term Frequency-Inverse Document Frequency) alapú súlyozásos módszert alkalmaztam. Ez a technika lehetővé tette, hogy meghatározzam az absztraktok relevanciáját a kutatás szempontjából [3]. A TF-IDF módszer során két kulcsszólistát hoztam létre: az egyik a mezőgazdaság (pl. "agriculture", "precision agriculture", "IoT"), a másik pedig a kiberbiztonság (pl. "cybersecurity", "data security", "malware") témáját reprezentálta. Ezek segítségével kiszámítottam a szakirodalmi absztraktok mezőgazdasági és kiberbiztonsági relevanciáját külön-külön, majd egy kombinált relevancia pontszámot hoztam létre, amely figyelembe vette mindkét terület súlyát.

Mivel kezdetben nem tudtam eldönteni, hogy milyen küszöbértéket (threshold) válasszak, ezért először ellenőriztem a relevancia pontszámok eloszlását. Az eloszlás elemzése azt mutatta, hogy a pontszámok medián értéke 0,5 körül van, a maximum 1.36.

A szakirodalmak szűkítésére különböző küszöbértékeket teszteltem a kombinált relevancia pontszám (TF-IDF) alapján, hogy meghatározzam az optimális értéket a releváns tanulmányok kiválasztásához. Az elemzés során a küszöbértékeket fokozatosan növeltem, 0,1-től 1,3-ig terjedő lépésekben, és megvizsgáltam, hogy az egyes küszöbök mellett mennyi szakirodalom maradt meg a vizsgálathoz. Az eredmények azt mutatták, hogy alacsonyabb küszöbértékek (pl. 0,1 vagy 0,3) esetén a megtartott szakirodalmak száma túl magas volt (491 absztrakt), míg magasabb küszöbértékek (pl. 1,2 vagy 1,3) mellett már túlságosan szűk listát kaptam.

*DOI: 10.21791/IJEMS.2025.03.*

A legjobb egyensúlyt az 1,03-as küszöbérték biztosította, amely 95 releváns szakirodalmat tartott meg a további elemzéshez. Ez az érték lehetővé tette, hogy a kombinált relevancia pontszám alapján kizárjam azokat a tanulmányokat, amelyek kevésbé kapcsolódtak szorosan mind a kiberbiztonság, mind a mezőgazdaság témájához, ugyanakkor elegendő számú tanulmányt hagyott meg a mélyebb elemzéshez. Az 1,03-as küszöbérték tehát biztosította, hogy a kutatásomhoz legjobban illeszkedő tanulmányokat válasszam ki.

A következő lépésben megkíséreltem hozzáférni a teljes szövegekhez, azonban az elérhetőség korlátai miatt csak 49 tanulmányhoz tudtam biztosítani a hozzáférést. Ezek a tanulmányok a legfontosabbak abból a szempontból, hogy átfogó képet nyújtsanak mind a kiberbiztonság, mind a mezőgazdaság területén releváns problémákról és megoldásokról. A 49 teljes szövegű tanulmányra koncentrálva folytattam a kutatást. A tartalmi áttekintés eredményeként 40 olyan tanulmányt határoztam meg, amelyek a kutatás szempontjából relevánsnak bizonyultak.

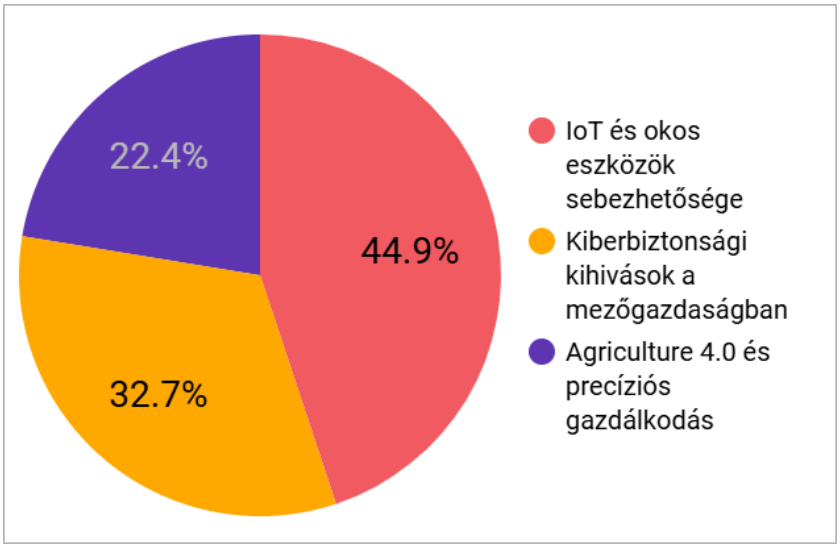
A teljes szövegű szakirodalmak tematikus megoszlása alapján jól látható, hogy a kutatási fókusz elsősorban az IoT és okos eszközök sebezhetőségéhez kapcsolódik, amely a vizsgált tanulmányok 44,9%-át teszi ki. Ez azt jelzi, hogy az IoT-eszközök térnyerése a mezőgazdaságban kiemelt figyelmet igényel a biztonsági kockázatok szempontjából. Az automatizált rendszerek, szenzorok és okos eszközök széles körű alkalmazása jelentős hatékonyságnövelést eredményez, ugyanakkor új típusú fenyegetettségeket is hordoz, amelyeket a szakirodalom alaposan elemez. A tanulmányok a sebezhetőségi tényezők részletezésére, az IoT-alapú támadások módszereire és azok megelőzési lehetőségeire koncentrálnak.

A kiberbiztonsági kihívások a mezőgazdaságban kategória a tanulmányok 32,7%-át fedi le, amely azt mutatja, hogy a mezőgazdasági vállalkozások számára a digitális fenyegetések felismerése és kezelése alapvető kihívást jelent. A kutatások ebben a témakörben különös hangsúlyt fektetnek az adatszivárgások megelőzésére, az infrastruktúra védelmére és a tudatosság növelésére. Ezen kihívások között szerepelnek a rosszindulatú támadások, például a zsarolóvírusok és szolgáltatásmegtagadási (DDoS) támadások, amelyek komoly üzleti kockázatot jelenthetnek az ágazat szereplői számára. Az elemzett tanulmányok rávilágítanak arra, hogy a megfelelő kiberbiztonsági stratégiák hiánya hosszú távon jelentős gazdasági és működési következményekkel járhat a vállalkozások számára.

A fennmaradó 22,4%-ot az Agriculture 4.0 és precíziós gazdálkodás kategóriába sorolt tanulmányok teszik ki, amelyek az új digitális technológiák mezőgazdaságban történő alkalmazásának biztonsági aspektusaira helyezik a hangsúlyt. A precíziós gazdálkodás és az automatizált mezőgazdasági rendszerek egyre nagyobb szerepet kapnak az élelmiszer-termelés hatékonyságának javításában, azonban ezek a rendszerek érzékeny adatokkal dolgoznak, és komplex hálózati kapcsolatokon keresztül működnek, amelyek jelentős sebezhetőséget hordoznak magukban. [12] A tanulmányok szerint az ilyen rendszerek védelme érdekében szükség van megfelelő titkosítási eljárásokra, adatvédelmi protokollokra, valamint az alkalmazott technológiák folyamatos biztonsági auditálására. Az

*DOI: 10.21791/IJEMS.2025.03.*

eredmények hangsúlyozzák, hogy az adatok integritásának és bizalmasságának biztosítása alapvető követelmény a fenntartható és biztonságos mezőgazdasági működés szempontjából.




*4.ábra: A teljes szövegű szakirodalmak tematikus megoszlása*
*Forrás: Saját készítés*

A 40 teljes szövegű tanulmányt megvizsgáltam a kutatás főbb kérdéseire való relevancia alapján is.

Az eredmény szerint az első kutatási kérdésre (Q1) összesen 38 szakirodalmi cikk, míg a második kérdésre (Q2) 34 szakirodalmi cikk azonosítható relevánsként a teljes szöveg elemzése alapján.

Q1: Hogyan hat az IoT-eszközök mezőgazdasági alkalmazása a kiberbiztonsági kihívásokra?

Q2: Milyen típusú kiberfenyegetések érintik a leginkább a mezőgazdaságot?

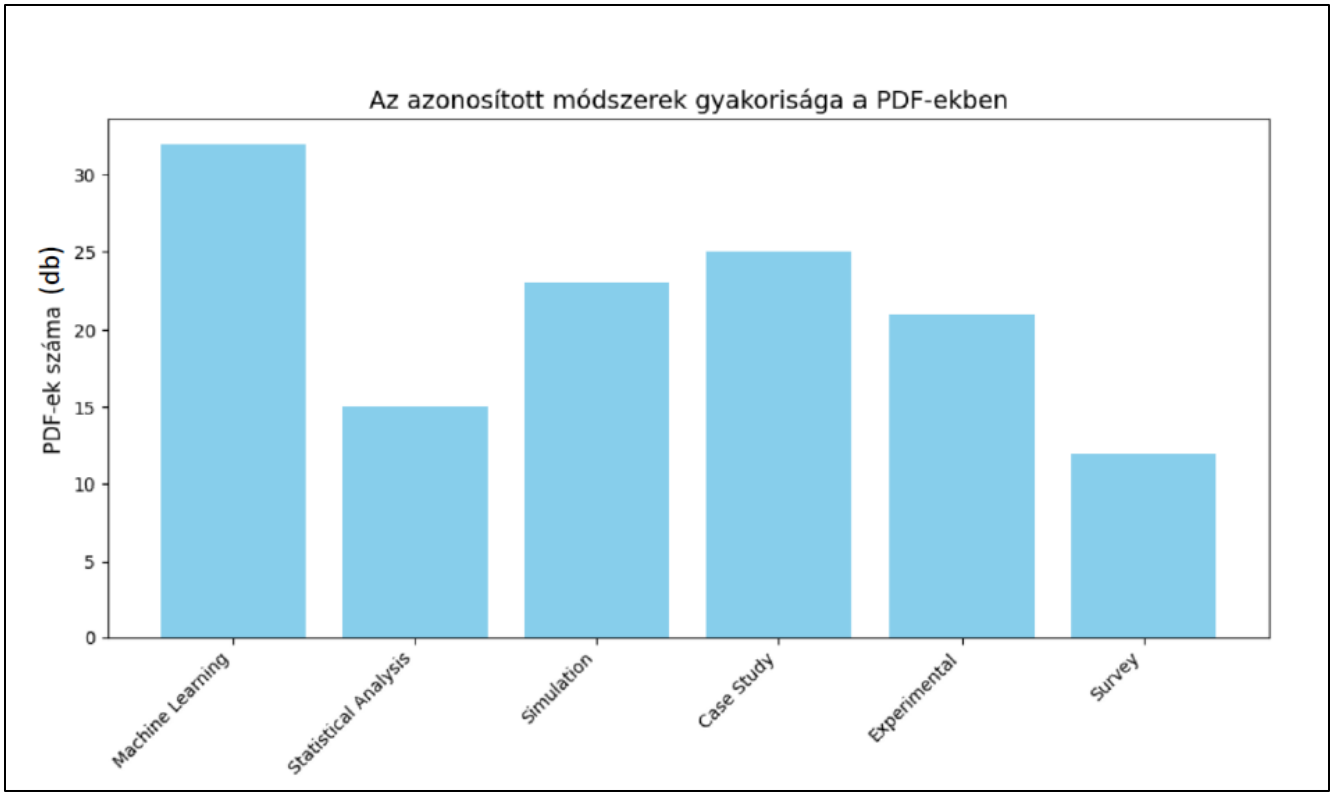
| | Kutatási kérdés | Szakirodalmak száma ▾ |
|---|---|---|
| 1. | Q1 | 38 |
| 2. | Q2 | 34 |

1 - 2 / 2 < >

*5.ábra: A kutatási kérdések alapján relevánsnak azonosítható szakirodalmak*
*Forrás: Saját készítés*

A teljes szövegek elemzését követően a cikkeket módszertani szempontból csoportosítottam, hogy átfogó képet kapjak az egyes tanulmányok által alkalmazott kutatási megközelítésekről. Az elemzés során kulcsszavak segítségével azonosítottam a tanulmányokban használt módszereket, mint például a gépi tanulás, a statisztikai elemzés, a szimuláció, esettanulmányok, felmérések és kísérleti kutatások. Ehhez egy Python-alapú szövegelemzési eljárást alkalmaztam, amely képes volt a PDF-ekből automatikusan kinyerni a releváns információkat, majd tematikusan csoportosítani azokat. Az elemzés eredménye a 6. ábrán látható.

*DOI: 10.21791/IJEMS.2025.03.*




*6.ábra: Módszerek gyakorisága*

*Forrás: Saját készítés*

Az elemzett tanulmányok módszertani megoszlása alapján a gépi tanulás (Machine Learning) a leggyakrabban használt megközelítés, amely kiemelkedik a kutatási spektrumból. Szorosan követi a szimuláció (Simulation) és az esettanulmányok (Case Study), míg a kísérleti kutatások (Experimental) és a statisztikai elemzések (Statistical Analysis) szintén jelentős részt képviselnek. A felmérések (Survey) alacsonyabb aránya arra utal, hogy ezek kevésbé dominálnak a mezőgazdasági kiberbiztonság területén végzett kutatásokban.

# Összegzés és konklúzió

A kutatás átfogó képet nyújt a mezőgazdaság digitalizációjának kiberbiztonsági kihívásairól, különös tekintettel az IoT-eszközök és a precíziós gazdálkodás biztonsági aspektusaira. Az irodalomkutatás során 1039 publikációt vizsgáltam meg, amelyek közül szisztematikus szűrési folyamat eredményeként 40 releváns tanulmányt azonosítottam. Az eredmények arra világítanak rá, hogy az IoT-eszközök sebezhetősége jelenti a legjelentősebb kihívást a mezőgazdasági digitalizáció során, a relevánsnak azonosított szakirodalom 44,9%-a foglalkozik ezzel a kérdéssel. Emellett a kiberbiztonsági kihívások (32,7%) és az Agriculture 4.0 technológiák biztonsági kérdései (22,4%) szintén jelentős szerepet kapnak a kutatásokban.

A módszertani elemzés feltárta, hogy a mezőgazdasági kiberbiztonsággal kapcsolatos kutatásokban a gépi tanulás, a szimulációs modellek és az esettanulmányok dominálnak, míg a kérdőíves és kísérleti kutatások kevésbé vannak jelen.

A kutatás eredményei továbbá azt mutatják, hogy a mezőgazdasági vállalkozások számára az információbiztonság tudatos kezelése elengedhetetlen, különösen az egyre komplexebb digitális

rendszerek térnyerésével. Ezek alapján egyértelművé vált, hogy a digitális transzformáció ugyan új lehetőségeket teremt az agrárszektor számára, de egyben növekvő kiberbiztonsági fenyegetésekkel is jár. Az IoT-eszközök biztonsági rései és a gyenge hitelesítési mechanizmusok jelentős kockázatot jelentenek a vállalkozások számára, amelyek az adatszivárgások és a kibertámadások fő célpontjaivá válhatnak.

További kutatási irányok

A mezőgazdasági kiberbiztonság területén született tanulmányok túlnyomórészt általános szinten tárgyalják a fenyegetéseket és megoldásokat, miközben kevés figyelmet fordítanak annak elemzésére, hogy az egyes gazdasági szereplők – például a nagyvállalatok és a kis- és középvállalkozások (KKV-k) – hogyan érintettek ezekben a kockázatokban. Ez egy fontos kutatási hiányosság, mivel az eltérő méretű és erőforrásokkal rendelkező szereplők különböző szinten vannak kitéve a kiberfenyegetéseknek. Például a nagyvállalatok gyakran rendelkeznek dedikált IT-biztonsági csapatokkal és fejlett védelmi rendszerekkel, amelyek mérsékelhetik a kiberfenyegetések hatásait. Ezzel szemben a KKV-k korlátozott erőforrásaik miatt sokkal sebezhetőbbek lehetnek, különösen az IoT-eszközök és digitális rendszerek sebezhetőségeivel szemben. Azonban jelenleg nincs átfogó kutatás, amely megvizsgálná, hogy ezek az eltérő kockázatok hogyan oszlanak meg, és milyen specifikus védelmi stratégiákra lenne szükség a különböző méretű szereplők számára.

Továbbá, az adatintegritás és az adatvédelmi kihívások további elemzése elengedhetetlen annak érdekében, hogy a mezőgazdasági digitalizáció biztonságosan és hatékonyan valósuljon meg. A jövőbeli kutatások során érdemes lenne kidolgozni olyan biztonsági keretrendszereket, amelyek segítik az agrárvállalkozásokat az IoT-eszközök biztonságos integrációjában és a fenyegetések hatékony kezelésében. Ezen túlmenően fontos lenne a mezőgazdasági termelők kiberbiztonsági tudatosságának növelését célzó stratégiák kidolgozása és az emberi tényező szerepének vizsgálata a kiberbiztonsági események vonatkozásában.

A további kutatási irányok között érdemes megfontolni a vizsgált tanulmányok relevanciájának mélyebb elemzését, amely során figyelembe lehet venni a publikációk minőségét meghatározó tényezőket, például az impakt faktort (IF) és a folyóiratok quartilis besorolását (Q érték). Az ilyen típusú értékelés hozzájárulhat a kutatási eredmények megbízhatóságának és hitelességének növeléséhez, valamint segíthet az azonosított szakirodalmi források tudományos súlyának pontosabb meghatározásában.

Összességében a kutatás rávilágított arra, hogy a mezőgazdasági kiberbiztonság egy komplex és multidiszciplináris terület, amely számos fejlesztést igényel mind technológiai, mind szervezeti szinten. Az elkövetkező években a kiberbiztonsági megoldások és stratégiák alkalmazásának optimalizálása kulcsfontosságú lesz a fenntartható és biztonságos mezőgazdasági digitalizáció érdekében.

# Hivatkozások

[1] B. Akhigbe, K. Munir, O. Akinadé, L. Akanbi, and L. Oyedele, "IoT Technologies for Livestock Management: A Review of Present Status, Opportunities, and Future Trends," *Big data and cognitive computing*, vol. 5, p. 10, 2021, doi: 10.3390/bdcc5010010.

[2] G. Rosline, P. Rani, and D. Rajesh, *Comprehensive Analysis on Security Threats Prevalent in IoT-Based Smart Farming Systems*. 2021, pp. 185–194.

[3] D. Gunawan, C. A. Sembiring, and M. A. Budiman, "The Implementation of Cosine Similarity to Calculate Text Relevance between Two Documents" , *Journal of physics: conference series,* vol. 978, no. 1, p. 012120, 2018, doi: 10.1088/1742-6596/978/1/012120.

[4] T. Gebremichael et al., "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access*, p. 1, 2020, doi: 10.1109/ACCESS.2020.3016937.

[5] W. Ali, M. Ali, M. Ahmad, S. Dilawar, A. Firdous, and A. Afzal, "Application of Modern Techniques in Animal Production Sector for Human and Animal Welfare," *Turkish Journal of Agriculture-Food Science and Technolog* , vol. 8, p. 457, 2020, doi: 10.24925/turjaf.v8i2.457-463.3159.

[6] O. A. Adebunmi, R. C. Njideka, and N. L. Eyo-Udo, "Cybersecurity in precision agriculture: Protecting data integrity and privacy", *International Journal of Applied Research in Social Sciences* vol. 5, no. 10, pp. 693–708, 2023, doi: 10.51594/ijarss.v5i10.1482.

[7] D. Moher et al., "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement", *Systematic reviews* vol. 4, no. 1, p. 1, 2015, doi: 10.1186/2046-4053-4-1.

[8] O. Adewusi, N. R. Chiekezie, and N. Eyo-Udo, "Securing smart agriculture: Cybersecurity challenges and solutions" in *IoT-driven farms*, vol. 15, no. 3, pp. 480–489, 2022, doi: 10.30574/wjarr.2022.15.3.0887.

[9] D. Cahyani and I. Patasik, "Performance comparison of TF-IDF and Word2Vec models for emotion text classification", *Bulletin of Electrical Engineering and Informatics* vol. 10, pp. 2780–2788, 2021, doi: 10.11591/eei.v10i5.3157.

[10] Adewusi, "Cybersecurity in precision agriculture: Protecting data integrity and privacy", *International Journal of Applied Research in Social Sciences* pp. 693–708, 2023, doi: 10.51594/ijarss.v5i10.1482.

[11] Maraveas, M. Rajarajan, K. G. Arvanitis, and A. Vatsanidou, "Cybersecurity threats and mitigation measures in agriculture 4.0 and 5.0", *Smart Agricultural Technology* vol. 9, p. 100616, 2024, doi: 10.1016/j.atech.2024.100616.

[12] H. T. Bui et al., "Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems", *Computers & Security* vol. 140, p. 103754, 2024, doi: 10.1016/j.cose.2024.103754.

[13] Adewusi, N. Chiekezie, and N. Eyo-Udo, "The role of AI in enhancing cybersecurity for smart farms", *World Journal of Advanced Research and Reviews* vol. 15, pp. 501–512, 2022, doi: 10.30574/wjarr.2022.15.3.0889.

[14] Nobles, D. Burrell, T. Waller, and A. Cusak, "Food Sustainability, Cyber-Biosecurity, Emerging Technologies, and Cybersecurity Risks in the Agriculture and Food Industries", *International Journal of Environmental Sustainability and Green Technologies (IJESGT)* vol. 13, pp. 1–17, 2022, doi: 10.4018/IJESGT.309744.

*DOI: 10.21791/IJEMS.2025.03.*

[15] M. Ayaz, A. Uddin, Z. Sharif, A. Mansour, and el-H. Aggoune, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk", *IEEE Access* p. 1, 2019, doi: 10.1109/ACCESS.2019.2932609.