Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра мережевих та інтернет технологій

ЗАТВЕРДЖУЮ

завідувач кафедри

мережевих та інтернет технологій

_____ Юрій КРАВЧЕНКО

«___»_____2023 року

КВАЛІФІКАЦІЙНА РОБОТА
БАКАЛАВРА
галузі знань 17 «Електроніка та телекомунікації»
за спеціальністю 172 «Телекомунікації та радіотехніка»
освітньо-професійна програма «Мережеві та інтернет технології»
на тему:

ВПРОВАДЖЕННЯ ІОТ-РІШЕНЬ ДЛЯ СИСТЕМ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

Дмитро МАНІЛО
(ім'я та ПРІЗВИЩЕ) _____ (підпис)

Виконав: студент групи МІТ-41

Керівник: доцент кафедри мережевих та інтернет технологій

к.т.н., Олена СТАРКОВА
(науковий ступень, вчене звання, ім'я та ПРІЗВИЩЕ) _____ (підпис)

Київ-2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій

ЗАТВЕРДЖУЮ

завідувач кафедри
мережевих та інтернет технологій
_____ Юрій КРАВЧЕНКО
«_____» _____2023 року

Кафедра мережевих та інтернет технологій

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Здобувачу вищої освіти Манілу Дмитру Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи:
Впровадження IoT-рішень для систем контролю та управління доступом.

затверджена на засіданні кафедри МІТ «07» грудня 2022 р. протокол №5
2. Термін здачі закінченої роботи «30» травня 2023 р.
3.Вихідні дані до проекту (роботи)

Симуляція в Cisco Packet Tracer

4. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити, обсяг – 35-40 стор.)

Вступ

1. АНАЛІЗ ВАЖЛИВОСТІ IoT ТА МЕРЕЖ В ЖИТТІ ЛЮДИНИ

1.1 Аналіз концепції Інтернету речей

1.2 Мережі, які застосовуються в IoT

1.3 Аналіз корисності СКУД та доцільність технології

1.4 Можливі методи дослідження технології

2. СКУД ЯК ІННОВАЦІЙНА ТЕХНОЛОГІЯ

2.1 Історія розвитку початкових версій СКУД та їх аналогів

2.2 Види сучасних СКУД

2.3 Компоненти сучасних СКУД

2.4 Проблеми сучасних СКУД

2.5 Тенденції розвитку СКУД

2.6 Способи покращення СКУД та їх удосконалення

3. РЕАЛІЗАЦІЯ СИМУЛЯЦІЇ СКУД В CISCO PACKET TRACER

3.1 Підготовка до реалізації

3.2 Реалізація симуляції

Дата видачі завдання 30.01.2023

Керівник роботи Олена СТАРКОВА

(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання

Дмитро МАНІЛО

(підпис)

КАЛЕНДАРНИЙ ПЛАН ВИКОНАННЯ РОБОТИ

Номер	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Підготовчий	01.02.2023	
2	Розділ 1	01.03.2023	
3	Розділ 2	01.04.2023	
4	Розділ 3	16.05.2023	
5	Доповідь та слайди	30.05.2023	
6	Пояснювальна записка	30.05.2023	

Здобувач вищої освіти  Дмитро МАНІЛО

(підпис)

Керівник _____ Олена СТАРКОВА

(підпис)

РЕФЕРАТ

Пояснювальна записка: 57 с, 16 рис, 18 джерел.

Об’єкт дослідження: Системи контролю та управління доступом.

Мета роботи (дослідження): вивчення сучасних систем контролю та управління доступом та вдосконалення їх на основі концепції Інтернету речей.

Методи дослідження: структурний аналіз, моделювання системи за допомогою програми для симулювання мережевих пристроїв та протоколів і технологій.

В роботі проведено аналіз сучасних систем контролю та управління доступу, які доступні та відомі на даний момент. Також досліджено можливості Інтернету речей с точки зору удосконалення роботи СКУД.

Розроблено: моделі (симуляції) в програмі Cisco Packet Tracer.

Практичне значення роботи полягає у тому, що модель дозволяє наглядно продемонструвати роботу даних систем та на практиці розібратися яким чином можна удосконалити та покращити методи їх взаємодії та розширення їх застосування.

Результати здійснених у дипломному проекті досліджень можуть бути використані в дослідницьких роботах або наглядних посібниках роботи сучасних систем управління та контролю доступом.

Ключові слова: МЕРЕЖЕВІ ТЕХНОЛОГІЇ, СИМУЛЯЦІЯ, КОНТРОЛЬ ТА УПРАВЛІННЯ ДОСТУПОМ, СИСТЕМА, ІОТ, ПЕРЕДАЧА ІНФОРМАЦІЇ, БЕЗПЕКА, ПОЛІТИКА КОНТРОЛЮ ДОСТУПОМ.

ABSTRACT

Explanatory note: 57 p., 16 drawings, 18 sources.

Research object: Access control and management systems.

The purpose of the work (research): study of modern access control and management systems and their improvement based on the concept of the Internet of Things.

Research methods: structural analysis, modeling systems using programs for modeling network devices and protocols and technologies.

The paper analyzes modern access control and management systems that are available and known at the moment. The possibilities of the Internet of Things from the point of view of improving the operation of the EMS were also investigated.

Developed: models (simulations) in the Cisco Packet Tracer program.

The practical significance of the work arises from the fact that the model allows you to visually demonstrate the operation of the data system and to understand in practice how to improve and improve the methods of their interaction and the expansion of their application.

The results of research valid in the diploma project can be used in research papers or visual manuals of the operation of a modern system of management and access control.

Keywords: NETWORK TECHNOLOGIES, SIMULATION, ACCESS CONTROL AND MANAGEMENT, SYSTEM, IoT, INFORMATION TRANSFER, SECURITY, ACCESS CONTROL POLICY.

ЗМІСТ

ВСТУП

Інтернет речей (IoT) є невід'ємною частиною сучасного суспільства, відкриваючи перед людством нові горизонти можливостей та розширюючи вже відомі області. Завдяки IoT, ми можемо побудувати мережі, які автоматизують рутинні роботи, які колись потребували нашої особистої уваги та зусиль. Це можна назвати новою ерою у розвитку технологій, оскільки IoT привносить інноваційні підходи та змінює наше сприйняття роботи та повсякденного життя.

Одним з застосувань IoT, яке має значний потенціал і практичне значення, є впровадження IoT рішень у системи контролю та управління доступом. Традиційно, системи контролю доступу використовуються для забезпечення безпеки та обмеження доступу до приміщень, об'єктів або ресурсів. Однак, за допомогою IoT технологій, ці системи стають ще більш ефективними, гнучкими та інтелектуальними.

Завдяки IoT, доступ контролю може бути реалізований за допомогою різноманітних пристроїв, таких як карт-рідери, біометричні сканери, сенсори руху та інші "розумні" пристрої, які підключаються до мережі Інтернет. Це дозволяє створити комплексну систему контролю доступу, яка забезпечує точність, швидкість та безпеку.

Одним з ключових переваг IoT в системах контролю доступу є можливість віддаленого керування та моніторингу. За допомогою смартфонів або комп'ютерів, користувачі можуть віддалено керувати доступом до приміщень, стежити за журналами входів-виходів, налаштовувати права доступу та отримувати повідомлення про неправильні спроби або незвичайну активність. Це не тільки забезпечує зручність, але і сприяє оперативній реакції на потенційні загрози та ускладнює нелегальний доступ.

Ще одна сильна сторона IoT в системах контролю доступу полягає в їх гнучкості та легкій масштабованості. Системи IoT можуть бути розгорнуті та

розширені в залежності від потреб організації або об'єкту. Нові пристрої можуть бути додані до мережі без значних зусиль та затрат, що дозволяє підлаштовувати систему під зростаючі вимоги та змінні потреби.

Нещодавні технологічні розробки в галузі IoT дозволяють впроваджувати аналітику та інтелектуальні алгоритми в системи контролю доступу. Завдяки цьому, системи можуть виявляти незвичайну активність, розпізнавати образи, ідентифікувати особу за мімікою або голосом, а також прогнозувати поведінку та аналізувати дані для покращення ефективності та безпеки.

У підсумку, впровадження рішень Інтернету речей в системи контролю та управління доступом відкриває нові можливості для підвищення безпеки, ефективності та зручності. За допомогою IoT, створюються інтелектуальні мережі, які дозволяють автоматизувати рутинні процеси, забезпечують гнучкість, масштабованість та віддалене керування. Такі рішення не тільки сприяють збереженню часу та зусиль, але й підвищують рівень безпеки та контролю в різних сферах діяльності, починаючи від підприємств та комерційних приміщень до житлових комплексів та офісів.

РОЗДІЛ 1. АНАЛІЗ ВАЖЛИВОСТІ IoT ТА МЕРЕЖ В ЖИТТІ ЛЮДИНИ

1.1 Аналіз концепції Інтернету речей

IoT, або Інтернет речей, — це концепція, яка стосується взаємозв'язку повсякденних об'єктів або «речей» через Інтернет. Він передбачає вбудовування датчиків, програмного забезпечення та підключення до фізичних пристроїв, що дозволяє їм збирати та обмінюватися даними. Ці підключені пристрої можуть варіюватися від побутової техніки та переносних пристроїв до промислового обладнання та інфраструктури.

IoT — це мережа фізичних пристроїв, транспортних засобів, будівель та інших об'єктів, у які вбудовано датчики, програмне забезпечення та підключення до мережі, що дозволяє їм збирати та обмінюватися даними.

Пристрої IoT підключаються до Інтернету або інших мереж, що дозволяє їм спілкуватися один з одним і з користувачами. Це підключення може бути дротовим або бездротовим, включаючи такі технології, як Wi-Fi, Bluetooth, стільникові мережі та глобальні мережі.

Основна частина ристроїв IoT оснащені різними датчиками, які збирають дані з навколишнього середовища. Ці датчики можуть вимірювати такі параметри, як температура, вологість, освітленість, рух тощо, залежно від конкретного застосування.

Пристрої IoT використовують різні протоколи зв'язку для обміну даними та взаємодії з іншими пристроями чи системами. Серед поширених протоколів MQTT, CoAP, HTTP та Zigbee.

IoT має застосування в різних областях, включаючи розумні будинки, охорону здоров'я, сільське господарство, транспорт, виробництво, управління енергією та моніторинг навколишнього середовища. Це забезпечує автоматизацію, моніторинг і контроль фізичних процесів, що сприяє підвищенню ефективності, продуктивності та зручності.

Безпека Інтернету речей є критичною проблемою через величезну кількість взаємопов’язаних пристроїв і конфіденційний характер зібраних даних. Захист цілісності даних, конфіденційності та приватності має важливе значення для запобігання несанкціонованому доступу та неправильному використанню систем IoT.

Оскільки IoT продовжує розвиватися, докладаються зусилля для встановлення стандартів і забезпечення сумісності між пристроями різних виробників. Стандартизація забезпечує повну інтеграцію, обмін даними та сумісність між різними платформами та екосистемами IoT.

Очікується, що зростання IoT продовжуватиметься швидким темпом із збільшенням кількості пристроїв і програм. Нові тенденції включають периферійні обчислення, де обробка даних здійснюється ближче до джерела, і підключення 5G, яке пропонує більш високу швидкість і меншу затримку для покращеного досвіду IoT.

У сфері технологічних досягнень Інтернет речей (IoT) став трансформаційною силою, яка революціонізує численні аспекти людського життя. Завдяки безперебійному підключенню та сумісності IoT проклав шлях для чудових оновлень у різних галузях і областях. В даному розділі досліджується значення IoT, його вплив на різні сектори та величезний потенціал, який він має для покращення якості людського існування.

Інтеграція IoT зробила революцію в галузях, запропонувавши незрівнянні покращення в таких сферах, як охорона здоров’я, виробництво, сільське господарство, транспорт та енергетика. Поєднуючи цифрові технології з фізичними об’єктами, IoT підвищив операційну ефективність, знизив витрати та розширив можливості процесів прийняття рішень.

В основі IoT лежить здатність підключатися (мати сумісність) та бездоганно взаємодіяти між пристроями, системами та платформами. Це полегшує обмін даними в режимі реального часу, забезпечуючи покращений зв’язок і співпрацю між

різними компонентами IoT. Таке підключення має вирішальне значення для досягнення спільних цілей і використання справжнього потенціалу IoT.

Пристрої IoT, оснащені датчиками, генерують величезні обсяги даних, забезпечуючи цінну інформацію за умови ефективного аналізу. Цей підхід, що керується даними, дозволяє компаніям і організаціям приймати обґрунтовані рішення, оптимізувати процеси та покращувати загальну продуктивність. Аналіз даних став вирішальним фактором у використанні можливостей IoT.

Інтернет речей породив концепцію розумних міст, де взаємопов’язані пристрої та інфраструктура сприяють ефективному управлінню ресурсами, оптимізованому транспортному потоку та покращенню громадських послуг. Віддаючи пріоритет стійкості та зв’язку, розумні міста прагнуть підвищити якість життя та створити зручніше для життя середовище.

Вплив Інтернету речей на охорону здоров’я є суттєвим, що дає постачальникам медичних послуг можливість революціонізувати лікування пацієнтів, віддалений моніторинг і діагностику. Від портативних пристроїв, що відстежують життєво важливі показники, до підключеного медичного обладнання, IoT забезпечує персоналізовані та проактивні медичні послуги, що сприяє кращим результатам для пацієнтів і підвищенню ефективності надання медичних послуг.

Інтернет речей зробив революцію в сільському господарстві завдяки технологіям точного землеробства. Датчики та виконавчі механізми, підключені до платформ IoT, надають дані в реальному часі про вологість ґрунту, погодні умови та здоров’я врожаю, що дозволяє фермерам приймати рішення на основі даних. Це сприяє оптимальному вирощуванню врожаю, зменшує втрату ресурсів і покращує практику сталого землеробства.

IoT відіграє життєво важливу роль в управлінні та збереженні енергії. Завдяки інтелектуальним лічильникам, підключеним приладам і інтелектуальним енергетичним мережам стає можливим моніторинг і оптимізація споживання в реальному часі. Інтеграція відновлюваних джерел енергії полегшується, що

призводить до зниження витрат, підвищення енергоефективності та більш сталого підходу до споживання енергії.

Системи з підтримкою Інтернету речей значно покращили безпеку в різних доменах. Інтелектуальні камери спостереження, системи контролю доступу та підключені домашні пристрої безпеки забезпечують моніторинг у реальному часі, раннє виявлення загроз і можливості дистанційного керування. Ці досягнення забезпечують безпеку людей, власності та критичної інфраструктури.

Транспорт і логістика стали свідками помітних покращень завдяки технологіям Інтернету речей. Підключені транспортні засоби, розумні логістичні рішення та системи оптимізації маршрутів підвищують ефективність, зменшують споживання палива та покращують загальну роботу ланцюга поставок. Відстеження товарів у режимі реального часу та ефективне управління транспортуванням стали можливими, що сприяє підвищенню продуктивності.

Інтеграція IoT стимулює інновації та економічне зростання, сприяючи створенню нових бізнес-моделей, створенню робочих місць і підприємницьким можливостям. IoT відкриває двері для проривних технологій і досягнень у сфері штучного інтелекту, аналізу великих даних і автоматизації. Це рухає суспільство до більш пов’язаного, стійкого та технологічно розвиненого майбутнього.

IoT — це чудовий технологічний прогрес, який має величезний потенціал революціонізувати різні аспекти людського життя. Його вплив поширюється на промисловість, міста, охорону здоров’я, сільське господарство, енергетику та транспорт. Забезпечуючи безперебійне підключення, розширений аналіз даних і вдосконалену автоматизацію, IoT проклав шлях для масштабних оновлень у прагненні людства до прогресу та сталого розвитку. Оскільки ми продовжуємо досліджувати та використовувати потужність IoT, на нас чекає майбутнє, наповнене безпрецедентними можливостями.

Підсумовуючи, можна відокремити одні з найважливіших галузей (та їх приклади в житті), які IoT революціонізує, є:

Охорона здоров’я: портативні пристрої з підтримкою Інтернету речей, такі як фітнес-трекери та розумні годинники, дозволяють людям відстежувати параметри свого здоров’я та обмінюватися даними з постачальниками медичних послуг для дистанційного моніторингу та персоналізованого догляду. Пристрої Інтернету речей дозволяють постачальникам медичних послуг дистанційно контролювати життєво важливі показники та стан здоров’я пацієнтів, скорочуючи відвідування лікарень і забезпечуючи проактивне управління доглядом. Дозатори таблеток із підтримкою Інтернету речей нагадують пацієнтам про необхідність прийняти ліки та повідомляють опікунів або медичних працівників у разі пропуску прийому доз.

Виробництво: розумні фабрики використовують датчики IoT для збору даних у реальному часі про продуктивність машин, оптимізації виробничих процесів, скорочення часу простою та підвищення загальної ефективності.

Сільське господарство: Іригаційні системи на основі Інтернету речей використовують датчики вологості ґрунту та погодні дані для автоматизації поливу, гарантуючи, що культури отримають потрібну кількість води в потрібний час, що призводить до підвищення врожайності та економії води.

Транспорт: підключені до Інтернету речей транспортні засоби та логістичні системи дозволяють відстежувати відправлення в реальному часі, оптимізувати маршрути, скорочувати час доставки та покращувати загальне управління ланцюгом поставок.

Підключення та сумісність також грає значну роль в важливості даної технології:

Розумний дім: такі пристрої IoT, як інтелектуальні термостати, системи освітлення та голосові помічники, можна безперешкодно підключати та керувати ними через уніфіковану платформу, що дозволяє користувачам ефективно керувати своїми будинками.

Промислова автоматизація: IoT дозволяє різним промисловим машинам і системам спілкуватися та координувати свої дії, оптимізуючи робочі процеси та сприяючи ефективним процесам автоматизації.

Розумні міста: мережі IoT об’єднують різні міські системи, такі як світлофори, управління відходами та енергетичні мережі, забезпечуючи ефективний розподіл ресурсів і покращуючи загальну якість життя громадян.

Також, інтернет речей допомагає покращити збір і аналіз даних на прикладі:

Роздрібна торгівля: маяки та датчики на основі Інтернету речей у магазинах роздрібної торгівлі збирають дані про поведінку та вподобання клієнтів, забезпечуючи персоналізовані маркетингові кампанії та покращуючи досвід покупок.

Енергоменеджмент: інтелектуальні лічильники, встановлені в будинках і на підприємствах, збирають дані про споживання енергії в реальному часі, що дозволяє користувачам аналізувати свої моделі споживання та приймати обґрунтовані рішення щодо енергоефективності.

Приклади розумних міст, які використовують масово інтернет речі:

Іспанія, Барселона впровадила системи на основі Інтернету речей для розумного паркування, управління відходами та моніторингу енергоспоживання, оптимізуючи розподіл ресурсів і сприяючи екологічним практикам.

В Сінгапурі, датчики та камери з підтримкою Інтернету речей контролюють різні аспекти міста, зокрема затори, якість повітря та управління відходами, щоб підвищити якість міського життя.

Покращене управління енергією:

Розумні електромережі: пристрої та датчики IoT контролюють розподіл енергії, оптимізуючи виробництво та передачу електроенергії, зменшуючи втрати енергії та забезпечуючи інтеграцію відновлюваних джерел енергії.

Термостати Nest: ці розумні термостати вивчають температурні уподобання користувачів і автоматично регулюють нагрівання та охолодження, що веде до економії енергії та зменшення рахунків за комунальні послуги.

Покращена безпека та захист:

Системи безпеки розумного дому: підключені до Інтернету речей камери безпеки, датчики руху та дверні замки дозволяють власникам будинків дистанційно контролювати та контролювати безпеку свого будинку, підвищуючи безпеку та забезпечуючи спокій.

Промислові об’єкти: системи відеоспостереження на основі Інтернету речей із відео аналітикою та контролем доступу допомагають забезпечити безпеку працівників, активів і критичної інфраструктури.

1.2 Мережі, які застосовуються в IoT

Дротові мережі відіграють важливу роль у підключенні пристроїв Інтернету речей, особливо в промислових умовах і стаціонарних установках. Ethernet, широко поширена технологія дротової мережі, забезпечує надійне та високошвидкісне підключення. Він забезпечує стабільну магістраль для передачі даних між пристроями IoT і централізованими системами. Мережі Ethernet забезпечують низьку затримку, високу пропускну здатність і безпечну передачу даних, що робить їх ідеальними для вимогливих програм IoT.

Бездротові мережі всюдисущі в розгортанні IoT, що дозволяє пристроям спілкуватися без фізичних з'єднань. Вони, зазвичай, набагато зручніші у використанні та підключенні ніж дротові аналоги. Кілька бездротових технологій зазвичай використовуються в IoT:

Мережі Wi-Fi пропонують гнучке та високошвидкісне підключення для пристроїв IoT у будинках, офісах та громадських місцях. Wi-Fi забезпечує середовище локальної мережі (LAN), забезпечуючи безперебійну передачу даних і доступ до Інтернету для пристроїв у зоні дії.

Також не меншу роль відіграє технологія Bluetooth, яка широко використовується для зв'язку на короткій відстані між пристроями IoT. Він зазвичай використовується в переносних пристроях, системах домашньої автоматизації та програмах для моніторингу особистого здоров'я.

Zigbee — це малопотужна бездротова технологія, розроблена для додатків Інтернету речей, які вимагають тривалого часу автономної роботи та низької швидкості передачі даних. Він зазвичай використовується в пристроях розумного будинку, промисловій автоматизації та системах управління будівлями.

Пристрої IoT також можуть використовувати стільникові мережі, такі як 3G, 4G LTE та нові технології 5G. Стільникові мережі пропонують широке покриття, що

дозволяє пристроям Інтернету речей підключатися віддалено та працювати в різноманітних середовищах.

При проектуванні мережі IoT слід враховувати кілька факторів:

●Масштабованість: мережі Інтернету речей мають безперешкодно пристосовуватися до зростаючої кількості пристроїв. Архітектура мережі має бути масштабованою, щоб обробляти масштабні розгортання без шкоди для продуктивності.

●Безпека: пристрої IoT є потенційними цілями для кібератак. Надійні заходи безпеки, включаючи шифрування, автентифікацію та контроль доступу, мають вирішальне значення для захисту конфіденційних даних і забезпечення цілісності мережі.

●Надійність: програми IoT часто вимагають надійного підключення, щоб забезпечити безперебійну передачу даних. Для підтримки надійності необхідно впровадити резервування мережі, механізми відновлення після відмови та методи якості обслуговування (QoS).

●Низьке енергоспоживання: багато пристроїв IoT працюють від обмежених джерел живлення, таких як батареї. Енергоефективні протоколи та оптимізація мережі допомагають мінімізувати енергоспоживання та продовжити термін служби пристрою.

●Сумісність: мережі IoT часто складаються з пристроїв різних виробників. Забезпечення сумісності через стандартні протоколи та відкриті архітектури сприяє безперебійному зв’язку між пристроями та забезпечує легку інтеграцію з існуючими системами.

Мережі IoT утворюють основу пов’язаних екосистем, забезпечуючи безперебійний зв’язок і обмін даними між розумними пристроями. Дротові та бездротові мережі, включаючи Ethernet, Wi-Fi, Bluetooth, Zigbee і стільникові мережі, забезпечують підключення, необхідне для додатків IoT. Розробка та впровадження надійної мережі Інтернету речей передбачає врахування

масштабованості, безпеки, надійності, енергоспоживання та сумісності. Завдяки правильній мережевій інфраструктурі пристрої IoT можуть використовувати потужність підключення, щоб відкрити нові можливості та зробити революцію в галузях у всьому світі.

1.3 Аналіз корисності СКУД та доцільність технології

Мета дослідження систем контролю доступу полягає в тому, щоб зрозуміти, як вони працюють, які переваги вони надають і як їх можна вдосконалити, щоб якнайкраще відповідати потребам сучасних організацій. Системи контролю доступу важливі в сучасному світі, оскільки вони допомагають запобігти несанкціонованому доступу до конфіденційних даних, захищають фізичні активи від крадіжки чи пошкодження та забезпечують дотримання нормативних вимог.

Впроваджуючи системи контролю доступу, організації можуть зменшити ризик порушення безпеки, мінімізувати наслідки втрати або крадіжки даних і підтримувати безпечне робоче середовище для співробітників. Можна виділити декілька доводів, які підтверджують доцільність таких технологій як СКУД, а саме один з них є покращена фізична безпека, тобто системи контролю доступу є основоположними для підтримки безпеки в організаціях. Впроваджуючи надійні механізми аутентифікації та авторизації, системи контролю доступу запобігають неавторизованим особам отримати доступ до конфіденційних областей, систем або інформації. Вони служать критичним бар’єром проти фізичних і цифрових загроз, захищаючи активи, дані та інфраструктуру. Наступним не менш важливим чинником є зменшення можливих ризиків. СКУД допомагають організаціям зменшувати різні ризики, пов’язані з несанкціонованим доступом і витоком даних. Застосовуючи політики контролю доступу, організації можуть зменшити ймовірність внутрішніх і зовнішніх інцидентів безпеки, включаючи крадіжки, саботаж, витік даних і порушення конфіденційності. Цей проактивний підхід допомагає захистити репутацію та діяльність організації. Системи контролю доступу відіграють важливу роль у забезпеченні відповідності галузевим нормам і законам про конфіденційність. Багато нормативних положень, як-от GDPR (General Data Protection Regulation - Загальний регламент захисту даних) і HIPAA (Health Insurance Portability and Accountability Act - Закон про перенесення та підзвітність медичного страхування),

вимагають від організацій запроваджувати відповідні засоби контролю доступу для захисту конфіденційних даних і забезпечення конфіденційності. Системи контролю доступу полегшують зусилля з дотримання вимог і допомагають уникнути дорогих штрафів. Також, дані системи захищають інтелектуальну власність, обмежуючи доступ до конфіденційних документів, комерційних таємниць або конфіденційної інформації. Впроваджуючи детальну політику контролю доступу, організації можуть гарантувати, що лише авторизовані особи з законною потребою зможуть отримати доступ до критично важливих активів, зменшуючи ризик крадіжки інтелектуальної власності або несанкціонованого розголошення. Ще одна характеристика систем є забезпечення безпеки співробітників, запобігаючи проникненню неавторизованих осіб у зони обмеженого доступу. Обмежуючи доступ до безпечних зон, організації можуть мінімізувати ризик фізичних загроз, насильства на робочому місці та несанкціонованого доступу до потенційно небезпечного середовища чи обладнання.

1.4 Можливі методи дослідження технології

Щоб дослідити роботу систем контролю доступу, методи дослідження можуть включати моделювання за допомогою таких інструментів, як Cisco Packet Tracer або мережевих емуляторів для аналізу поведінки системи за різними сценаріями.

Інструменти, такі як журналювання та аудит, можна використовувати для моніторингу подій системи контролю доступу та відстеження дій користувачів для аналізу та дослідження.

Методи тестування безпеки, такі як тестування на проникнення та оцінка вразливості, можна використовувати для виявлення потенційних слабких місць або вразливостей у системах контролю доступу.

Дослідження існуючої літератури, включаючи наукові журнали, галузеві публікації та офіційні документи, може дати розуміння принципів проектування, міркувань реалізації та оцінки систем контролю доступу.

Опитування та інтерв'ю з галузевими експертами, професіоналами з безпеки та системними адміністраторами можуть зібрати знання з перших вуст і точки зору щодо практики системи контролю доступу, викликів і вдосконалень.

Порівняльний аналіз реалізації різних систем контролю доступу та тематичні дослідження можуть допомогти зрозуміти сильні сторони, обмеження та продуктивність різних підходів до контролю доступу.

Аналіз розгортання систем контролю доступу в реальному світі та їх вплив на безпеку, ефективність і взаємодію з користувачем може дати цінну інформацію для дослідження їхньої роботи.

Співпраця з професіоналами та експертами в галузі систем контролю доступу може сприяти глибшому розумінню, доступу до галузевих ідей і використанню їх досвіду в розслідуваннях.

Етичні міркування, питання конфіденційності та юридичні наслідки, пов'язані з системами контролю доступу, слід брати до уваги під час розслідування, щоб

забезпечити відповідність і відповідальне використання технології.

Використовуючи комбінацію цих методів і підходів, можна отримати повне розуміння систем контролю доступу та зробити внесок у їх вдосконалення та подальший прогрес у цій галузі.

РОЗДІЛ 2. СКУД ЯК ІННОВАЦІЙНА ТЕХНОЛОГІЯ

2.1 Історія розвитку початкових версій СКУД та їх аналогів

Історію розробки та модернізації систем контролю доступу можна простежити з давніх часів, коли люди вперше почали використовувати фізичні бар'єри та механізми для контролю доступу до певних областей або ресурсів. Протягом багатьох років системи контролю доступу значно вдосконалювалися, включаючи технологічні досягнення та вирішуючи нові проблеми безпеки.

●Стародавні та середні часи: системи контролю доступу в ранніх цивілізаціях покладалися на фізичні бар'єри, такі як стіни, ворота та охоронці для контролю доступу. Були представлені замки та ключі, а базові механізми розвивалися з часом.

●Промислова революція: з початком індустріалізації зросла потреба в системах контролю доступу. Механічні замки та ключі стали більш досконалими, включаючи складні механізми та ключові системи.

●Електронний контроль доступу: У середині 20 століття з'явилися електронні системи контролю доступу. Спочатку ці системи використовували ключ-карти та технологію магнітної смуги. Розробка безконтактних карток і зчитувачів забезпечила швидший і зручніший доступ.

●Комп'ютеризований контроль доступу: із розвитком комп'ютерних технологій у 1970-х роках системи контролю доступу почали інтегруватися з комп'ютерами. Це дозволило централізоване керування, бази даних користувачів і більш розширені методи автентифікації.

●Технологія смарт-карт: у 1990-х роках технологія смарт-карт набула популярності в системах контролю доступу. Смарт-карти містили вбудовані мікропроцесори та пам'ять, що забезпечувало підвищену безпеку та багатофункціональність.

●Біометрична автентифікація: Біометричні технології, такі як сканери відбитків пальців, розпізнавання райдужної оболонки ока та розпізнавання обличчя, були

інтегровані в системи контролю доступу в останні десятиліття. Біометрія забезпечує підвищену точність і зручність ідентифікації користувачів.

●Мобільний доступ: розвиток мобільних технологій призвів до інтеграції смартфонів у системи контролю доступу. Рішення для мобільного доступу використовують Bluetooth, NFC або Wi-Fi, щоб дозволити користувачам використовувати свої мобільні пристрої як облікові дані доступу.

●Хмарний контроль доступу: Хмарні обчислення зробили революцію в системах контролю доступу, забезпечивши централізоване адміністрування, віддалене керування та масштабованість. Хмарний контроль доступу дозволяє оновлювати в реальному часі, аналітику та інтегрувати з іншими системами.

●Інтеграція з IoT: Інтернет речей (IoT) дозволив системам контролю доступу підключатися до широкого кола пристроїв, включаючи датчики, виконавчі механізми та камери спостереження. Інтеграція IoT покращує можливості автоматизації, моніторингу та реагування.

●Розширені методи аутентифікації: системи контролю доступу продовжують розвиватися разом із удосконаленням методів аутентифікації, таких як двофакторна, багатофакторна та адаптивна, покращуючи безпеку та взаємодію з користувачем.

●Штучний інтелект і машинне навчання: інтеграція технологій штучного інтелекту (AI) і машинного навчання (ML) сприяє розробці більш інтелектуальних і адаптивних систем контролю доступу. AI/ML може аналізувати моделі поведінки користувачів, виявляти аномалії та забезпечувати профілактичні заходи безпеки.

●Міркування щодо кібербезпеки: оскільки системи контролю доступу стають все більш взаємопов’язаними, кібербезпека стала суттєвою увагою. Постійні оновлення та вдосконалення спрямовані на вирішення нових загроз, вразливостей і вимог відповідності.

Загалом, історія розвитку систем контролю доступу демонструє прогрес від простих фізичних бар’єрів до складних електронних і цифрових систем. Постійні оновлення та інтеграція з передовими технологіями спрямовані на підвищення

безпеки, зручності та масштабованості в контролі доступу до фізичних просторів і цифрових ресурсів.

2.2 Види сучасних СКУД

Сучасні системи контролю доступу — це рішення безпеки, які регулюють і керують входом і виходом осіб або організацій у фізичні простори, цифрові ресурси або мережі. Ці системи використовують передові технології та методології для забезпечення авторизованого доступу та запобігання несанкціонованому проникненню. Одні з основних типів СКУД є системи контролю фізичного доступу (PACS), яка керує фізичним доступом до будівель, приміщень або зон. Вони зазвичай використовують такі пристрої, як зчитувачі карток, клавіатури, біометричні сканери та електронні замки, щоб надати або заборонити доступ. Приклади таких систем:

●Платформа iCLASS SE від HID Global - Ця система поєднує зчитувачі карток, клавіатури та електронні замки для контролю доступу до будівель, приміщень і зон. Він підтримує різні карткові технології та пропонує розширені функції безпеки.

●Kisi - це хмарна система контролю доступу, яка використовує облікові дані смартфона та інтегрується з пристроями фізичного доступу, такими як пристрої для зчитування карток та електронні замки. Він надає можливості віддаленого керування та моніторингу в реальному часі.

Також ще один тип систем є логічні системи контролю доступу (LACS). Вони контролюють доступ до цифрових ресурсів, мереж або комп’ютерних систем. Покладаються на такі механізми аутентифікації, як імена користувачів, паролі, цифрові сертифікати або багатофакторну автентифікацію для перевірки облікових даних користувача. Приклади даних систем:

●Microsoft Active Directory - це широко використовуваний LACS, який керує доступом до комп’ютерних систем і ресурсів у мережі Windows. Він використовує імена користувачів/паролі та контроль доступу на основі груп.

●RSA SecurID - це рішення двофакторної автентифікації, яке поєднує імена користувачів/паролі з маркерами на основі часу або мобільними додатками. Він зазвичай використовується для безпечного віддаленого доступу до мереж і систем.

Мобільні системи контролю доступу використовують мобільні пристрої, такі як смартфони або переносні пристрої, як облікові дані доступу. Вони використовують такі технології, як Bluetooth, NFC або QR-коди, щоб забезпечити безконтактний доступ. Приклади систем з даним типом:

●Openpath пропонує мобільну систему контролю доступу, яка дозволяє користувачам відмикати двері за допомогою своїх смартфонів. Він використовує Bluetooth і хмарну технологію для безперебійного та безпечного доступу.

●SALTO KS (Ключі як послуга) надає перш за все мобільну систему контролю доступу, яка дозволяє користувачам використовувати свої смартфони для доступу. Він підтримує технологію NFC для безконтактного входу.

Хмарні системи контролю доступу зберігають дані контролю доступу та конфігурації в хмарі, що дозволяє віддалене керування та контроль доступу з будь-якого місця. Приклади:

●Brivo - це хмарне рішення для контролю доступу, яке дозволяє організаціям керувати дозволами доступу та контролювати діяльність із централізованої платформи. Він пропонує віддалений контроль доступу та інтеграцію з іншими системами безпеки.

●Genetec Synergis Cloud Link - це хмарна система контролю доступу, запропонована Genetec. Він забезпечує безпечне керування доступом, моніторинг подій і можливості звітування.

Біометричні системи контролю доступу використовують унікальні фізіологічні чи поведінкові характеристики, як-от відбитки пальців, сканування райдужної оболонки ока, розпізнавання обличчя чи розпізнавання голосу для підтвердження особи. Приклади систем:

●Suprema BioEntry W2 - це біометричний пристрій контролю доступу, який використовує розпізнавання відбитків пальців для автентифікації користувача. Він забезпечує високу точність і високу швидкість узгодження.

●FaceFirst - це система контролю доступу на основі розпізнавання облич, яка перевіряє особу людей шляхом аналізу рис обличчя. Він використовується в різних галузях для безпечного керування доступом.

Отже, можна зробити висновок, що сучасні СКУД мають значну різноманітність та можуть бути застосовані в різних ситуаціях залежно від функціональних потреб для успішної реалізації контролю відповідної системи чи організації.

2.3 Компоненти сучасних СКУД

Сучасні системи контролю доступу складаються з кількох важливих компонентів, які працюють разом, щоб забезпечити безпеку та ефективність контролю доступу. Ці компоненти включають:

1. Політики контролю доступу визначають правила та критерії, які керують доступом до ресурсів. Вони визначають, хто може отримати доступ до яких ресурсів, за яких умов і з якими дозволами. Політики контролю доступу мають важливе значення для дотримання вимог безпеки та керування привілеями користувачів.

2. Механізми автентифікації перевіряють особу користувачів, які намагаються отримати доступ до системи або ресурсів. Загальні методи автентифікації включають паролі, біометричні дані (наприклад, відбитки пальців або розпізнавання обличчя), смарт-карти та багатофакторну автентифікацію. Надійні механізми аутентифікації мають вирішальне значення для забезпечення доступу лише авторизованих осіб.

3. Механізми авторизації визначають, які дії або операції користувачеві дозволено виконувати після автентифікації. Він забезпечує дотримання правил контролю доступу та перевіряє, чи має користувач необхідні дозволи для виконання певних дій. Управління доступом на основі ролей (RBAC) і керування доступом на основі атрибутів (ABAC) є широко використовуваними моделями авторизації.

4. Керування користувачами передбачає створення, зміну та видалення облікових записів користувачів і пов’язаних з ними прав доступу. Він включає надання користувачам, деініціалізацію та керування життєвим циклом облікового запису. Керування користувачами забезпечує точне надання та скасування привілеїв доступу відповідно до організаційних ролей і обов’язків.

5. Керування обліковими даними передбачає безпечне зберігання, розповсюдження та перевірку облікових даних доступу. Він містить механізми безпечного зберігання паролів, керування ключами шифрування, видачі та

відкликання цифрових сертифікатів і забезпечення цілісності облікових даних доступу.

6. Механізми контролю доступу реалізують і забезпечують виконання політик контролю доступу. Вони гарантують, що запити на доступ оцінюються відповідно до визначених політик і що спроби несанкціонованого доступу відхиляються. Застосування контролю доступу може включати контроль на основі мережі, контроль на основі хоста або комбінацію обох.

7. Механізми аудиту та журналювання записують події та дії, пов’язані з контролем доступу, для цілей аудиту та судової експертизи. Вони збирають таку інформацію, як спроби входу, запити на доступ і зміни конфігурацій контролю доступу. Журнали аудиту мають вирішальне значення для моніторингу, виявлення порушень безпеки та розслідування інцидентів.

8. Сучасні системи контролю доступу часто інтегруються з фізичними компонентами безпеки, такими як камери спостереження, дверні замки та сигналізація. Інтеграція забезпечує комплексний підхід до безпеки, коли фізичні та цифрові засоби контролю доступу працюють разом, щоб забезпечити захист активів і об’єктів.

9. Централізовані платформи керування або програмне забезпечення забезпечують уніфікований інтерфейс для адміністрування та моніторингу систем контролю доступу. Вони дозволяють адміністраторам керувати обліковими записами користувачів, визначати політики контролю доступу, налаштовувати правила доступу та контролювати діяльність системи з централізованого місця.

10. Сучасні системи контролю доступу мають бути масштабованими та гнучкими, щоб відповідати мінливим потребам організацій. Вони повинні підтримувати додавання або видалення користувачів, розширення точок доступу та модифікацію політик контролю доступу без порушення загальної функціональності системи.

Дані компоненти разом сприяють надійності, ефективності та безпеці сучасних

систем контролю доступу. Кожен компонент відіграє вирішальну роль у забезпеченні належного доступу до ресурсів лише уповноважених осіб, зберігаючи при цьому конфіденційність, цілісність і доступність конфіденційної інформації та активів.

2.4 Проблеми сучасних СКУД

Незважаючи на те, що сучасні системи контролю доступу пропонують численні переваги, вони також стикаються з кількома викликами та проблемами, які організації та спеціалісти з безпеки мають вирішити. Ось деякі типові проблеми, пов’язані з сучасними системами контролю доступу:

●Вразливість до кібератак: оскільки системи контролю доступу все більше покладаються на цифрові технології, вони стають уразливими до кіберзагроз. Слабкі паролі, вразливість програмного забезпечення та неадекватні заходи безпеки можуть наражати системи контролю доступу на несанкціонований доступ або маніпуляції.

●Відсутність інтеграції: системи контролю доступу часто працюють у відсіках, що ускладнює їх інтеграцію з іншими системами безпеки, такими як камери спостереження або системи виявлення вторгнень. Ця відсутність інтеграції може обмежити загальну ефективність і координацію заходів безпеки.

●Комплексне керування. Управління системами контролю доступу, особливо у великих організаціях із великою кількістю користувачів і точок доступу, може бути складним. Це вимагає належного адміністрування, ініціалізації користувачів, керування політикою доступу та координації між кількома відділами чи місцями.

●Зручність для користувача та безпека: знайти правильний баланс між зручністю для користувача та безпекою є постійною проблемою. Надто суворі заходи безпеки можуть перешкодити взаємодії з користувачем, тоді як м’які заходи можуть поставити під загрозу безпеку. Знайти оптимальний баланс важливо, але складно.

●Високі витрати: Впровадження та підтримка надійних систем контролю доступу може бути дорогим, особливо для організацій із кількома точками доступу та складною інфраструктурою. Витрати включають апаратне забезпечення, ліцензії на програмне забезпечення, встановлення, технічне обслуговування та поточні оновлення системи.

●Помилкові спрацьовування та помилкові негативні результати: системи контролю доступу можуть генерувати помилкові спрацьовування (надання доступу неавторизованим особам) або помилкові негативі результати (відмова в доступі авторизованим особам), що призводить до незручностей, порушень безпеки або проблем з продуктивністю.

●Внутрішні загрози: незважаючи на системи контролю доступу, внутрішні загрози залишаються проблемою. Уповноважені особи зі зловмисними намірами можуть використовувати свої законні привілеї доступу, щоб порушити заходи безпеки та завдати шкоди організації.

●Питання фізичної безпеки. Хоча системи контролю доступу зосереджені на цифровому доступі, фізична безпека пристроїв та інфраструктури є не менш важливою. Фізичне втручання, викрадення облікових даних або обхід фізичних бар'єрів можуть знизити ефективність заходів контролю доступу.

●Проблеми конфіденційності: системи контролю доступу збирають і зберігають особисту інформацію, таку як облікові дані користувача та біометричні дані. Забезпечення належних заходів конфіденційності, захисту даних і дотримання правил конфіденційності має вирішальне значення для підтримки довіри користувачів.

●Масштабованість і гнучкість: системи контролю доступу повинні мати можливість адаптуватися до мінливих організаційних потреб, таких як додавання або видалення користувачів, коригування політики доступу або пристосування до мінливих вимог безпеки. Забезпечення масштабованості та гнучкості може бути складним завданням, особливо в складних середовищах.

●Навчання користувачів: Належна освіта та навчання користувачів є важливими для ефективного контролю доступу. Однак користувачі можуть бути недостатньо обізнаними щодо найкращих методів безпеки, стати жертвами атак соціальної інженерії або не дотримуватися політики безпеки, що може послабити загальну систему контролю доступу.

Вирішення цих проблем вимагає комплексного підходу, який поєднує технологічні досягнення, надійні заходи безпеки, обізнаність користувачів і навчання, регулярні аудити та оцінки, а також сильну увагу до управління ризиками та стратегій пом’якшення.

2.5 Тенденції розвитку СКУД

Професіонали в області систем контролю доступу передбачають кілька тенденцій і досягнень, які визначать майбутнє контролю доступу. Кілька ключових аспектів, на які звернули увагу експерти:

●Біометрична автентифікація. Очікується, що біометричні технології, такі як розпізнавання обличчя, сканування райдужної оболонки ока та розпізнавання голосу, відіграватимуть більш значну роль у системах контролю доступу. Покращення точності, швидкості та надійності підвищать безпеку та зручність для користувачів.

●Мобільний і хмарний доступ: інтеграція мобільних пристроїв і хмарних обчислень буде продовжувати розширюватися в системах контролю доступу. Облікові дані мобільного доступу, що зберігаються на смартфонах, у поєднанні з хмарним керуванням забезпечують гнучкість, масштабованість і зручність для користувачів і адміністраторів.

●Інтеграція Інтернету речей (IoT): Системи контролю доступу все більше інтегруватимуться з пристроями IoT для створення розумніших та більш пов’язаних середовищ. Датчики, приводи та камери спостереження IoT покращують автоматизацію, моніторинг у реальному часі та контекстний контроль доступу.

●Штучний інтелект і машинне навчання: технології AI (Artificial Intelligence) і ML (Machine Learning) покращать можливості систем контролю доступу. Ці технології можуть аналізувати поведінку користувачів, виявляти аномалії та забезпечувати проактивне виявлення загроз і реагування на них, підвищуючи загальну безпеку.

●Адаптивний і контекстний контроль доступу: системи контролю доступу стануть більш адаптивними, регулюючи привілеї доступу на основі контекстних факторів, таких як час, місцезнаходження, поведінка користувачів і рівні ризику. Цей динамічний підхід забезпечує відповідні дозволи доступу, одночасно

зменшуючи адміністративні витрати.

●Технологія блокчейн: блокчейн, з його децентралізованою та незмінною природою, має потенціал для підвищення безпеки та цілісності систем контролю доступу. Це може допомогти встановити довіру, запобігти неавторизованим змінам і оптимізувати процеси керування ідентифікацією.

●Інтеграція з системами фізичної безпеки: системи контролю доступу будуть додатково інтегровані з системами фізичної безпеки, такими як відеоспостереження та виявлення вторгнень. Ця інтеграція дозволяє більш комплексно відстежувати загрози, реагувати на інциденти та криміналістичний аналіз.

●Дизайн і досвід, орієнтований на користувача: майбутні системи контролю доступу нададуть пріоритет користувацькому досвіду, наголошуючи на інтуїтивно зрозумілих інтерфейсах, простих методах автентифікації та персоналізованих параметрах доступу. Дизайн, орієнтований на користувача, підвищить зручність використання, прийняття та загальну відповідність вимогам безпеки.

●Покращена аналітика даних і аналітика: системи контролю доступу використовуватимуть передові методи аналітики для отримання значущої інформації з журналів доступу, поведінки користувачів і системних подій. Ці відомості можуть інформувати про покращення безпеки, коригування політики та заходи відповідності.

●Більш суворі заходи кібербезпеки: у міру того, як ландшафт загроз розвиватиметься, системи контролю доступу застосовуватимуть суворіші заходи кібербезпеки. Це включає надійне шифрування, багатофакторну автентифікацію, безпечне керування обліковими даними та постійний моніторинг для виявлення інцидентів безпеки та реагування на них.

●Зауваження щодо відповідності та конфіденційності: системи контролю доступу відповідатимуть регулятивним вимогам, що змінюються, таким як закони про захист даних і конфіденційність. Технології підвищення конфіденційності, прозорі методи обробки даних і механізми згоди користувачів стануть невід’ємною

частиною майбутніх систем контролю доступу.

●Інтеграція з ідентифікацією та керуванням доступом (IAM): системи контролю доступу будуть більш легко інтегруватися з рішеннями IAM, забезпечуючи цілісний підхід до керування ідентифікацією користувачів, правами доступу та дозволами в різних системах і програмах.

Вищеперелічені тенденції вказують на майбутнє, коли системи контролю доступу стануть більш інтелектуальними, підключеними, зручними та адаптованими, пропонуючи покращену безпеку та досвід користувача в різноманітних середовищах. Однак важливо зазначити, що майбутнє систем контролю доступу буде формуватися прогресом технологій, зміною проблем безпеки, галузевими правилами та потребами організацій і користувачів

2.6 Способи покращення СКУД та їх удосконалення

Системи контролю доступу можна покращити шляхом включення передових технологій, таких як біометрична автентифікація, машинне навчання та штучний інтелект, для підвищення їх точності, швидкості та ефективності.

Ще один спосіб удосконалення систем контролю доступу — це використання багаторівневого підходу, який включає кілька рівнів захисту, таких як брандмауери, системи виявлення вторгнень і шифрування, щоб забезпечити комплексне та надійне рішення безпеки.

Організації також можуть покращити системи контролю доступу, проводячи регулярні аудити, оцінки вразливостей і тестування на проникнення, щоб виявити та усунути слабкі місця та вразливості безпеки.

Крім того, дослідження систем контролю доступу можуть допомогти організаціям зрозуміти вплив нових тенденцій, таких як Інтернет речей (IoT), на їхній рівень безпеки та визначити стратегії захисту пристроїв і даних IoT.

Проводячи дослідження систем контролю доступу, організації можуть залишатися на випередженні та завчасно протидіяти загрозам безпеці, допомагаючи захистити свої активи, репутацію та кінцевий результат.

Підсумовуючи, дослідження систем контролю доступу є важливими для розуміння переваг і обмежень цих технологій, визначення областей, які потребують удосконалення, а також для того, щоб бути в курсі останніх тенденцій безпеки та передового досвіду.

Розділ 3. РЕАЛІЗАЦІЯ СИМУЛЯЦІЇ СКУД В CISCO PACKET TRACER

3.1 Підготовка до реалізації

Для реалізації симуляції було взято Cisco Packet Tracer, так як він, має багатий функціонал та сам по собі простий у використанні інструмент для симуляції мереж та їх взаємодії. За основу для реалізації буде взято систему контролю фізичного доступу (PACS), адже вона є основним та поширеним на даний момент типом СКУД, також, в інструменті для мережевих симуляцій є потрібні для цього пристрої.

Пристрої, які будуть відігравати роль пристроїв в умовному офісі, а саме (Рисунок 3.1.1):

- Камери для нагляду
- Зчитувач карт
- Електронні двері
- Декілька карт
- Сирена
- Детектор руху
- Декілька світчів (Switch)
- Точка доступу (Access point)
- Комп’ютер інженера (або інший девайс який може підключитись до мережі та налаштувати правила взаємодії IoT пристроїв)
- Сервер

3.2 Реалізація симуляції

Для початку треба зробити логічну схему та розмістити всі потрібні для дослідження об’єкти на рисунку 3.1.1.

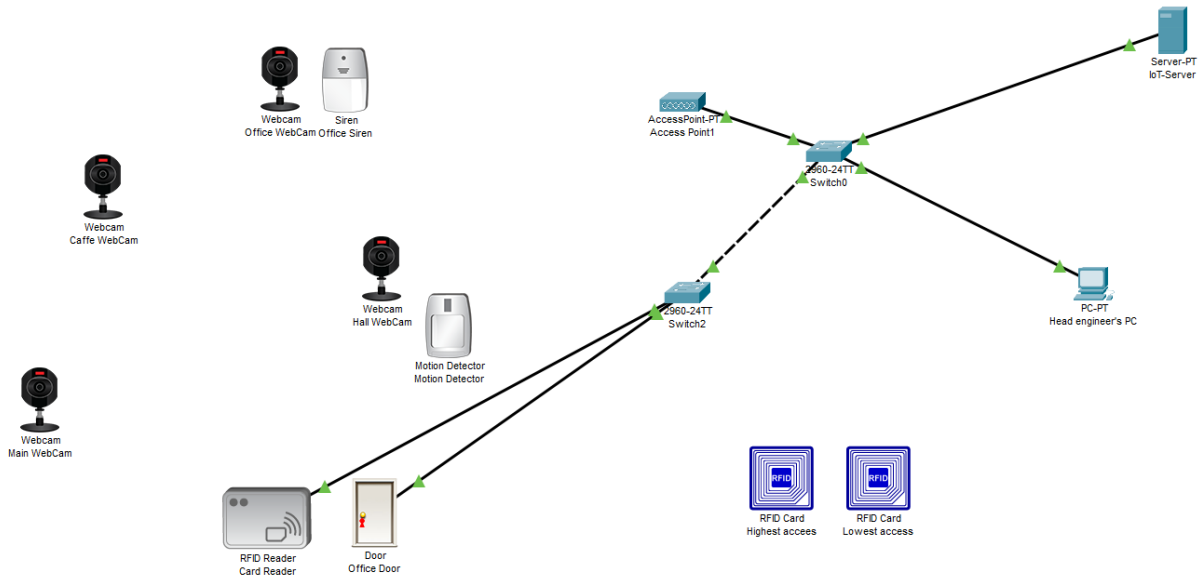

Рисунок 3.1.1 - Необхідні пристрої для симуляції (логічна топологія)

Після цього, можемо розмістити ці об’єкти на фізичній топології для максимального приближення до реальних умов (Рисунок 3.1.2):

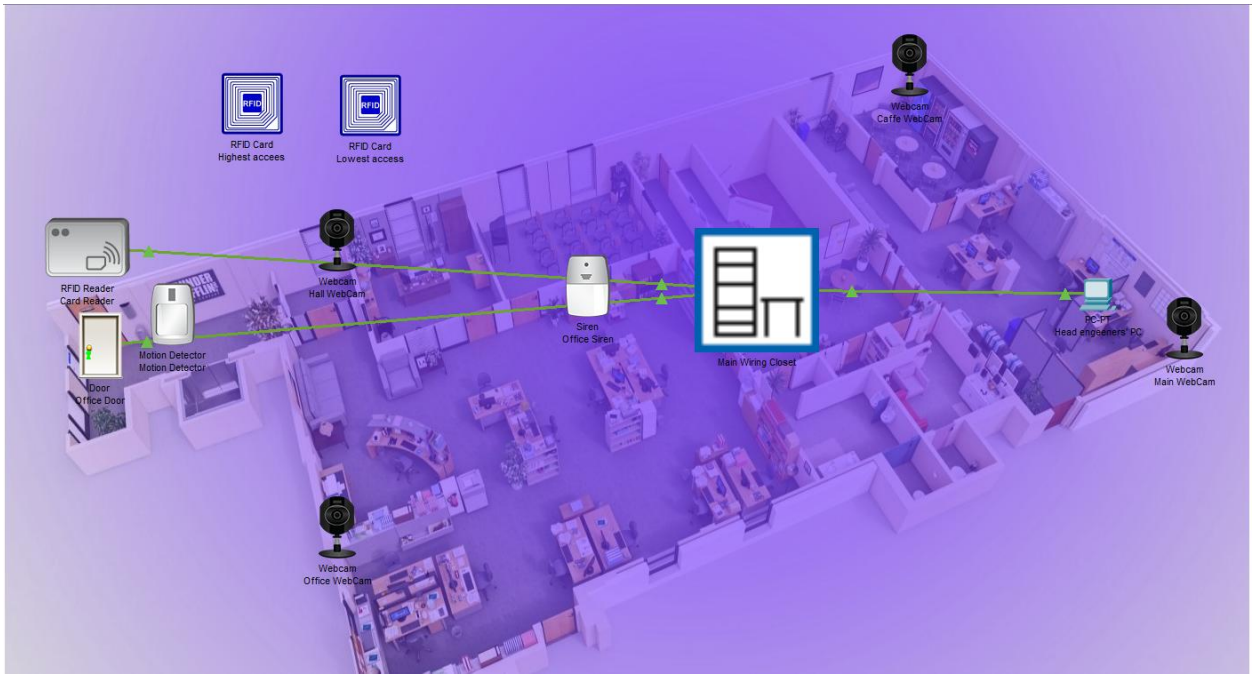

Рисунок 3.1.2 - Фізична топологія

Далі в IoT-сервері налаштуємо декілька сервісів, а саме:

●DHCP - (Dynamic Host Configuration Protocol) динамічна адресація пристроїв за допомогою протоколу (Рисунок 3.1.3)

●IoT-сервіс - буде використаний як ресурс на сервері, який буде керувати взаємодією між пристроями. (Рисунок 3.1.4)

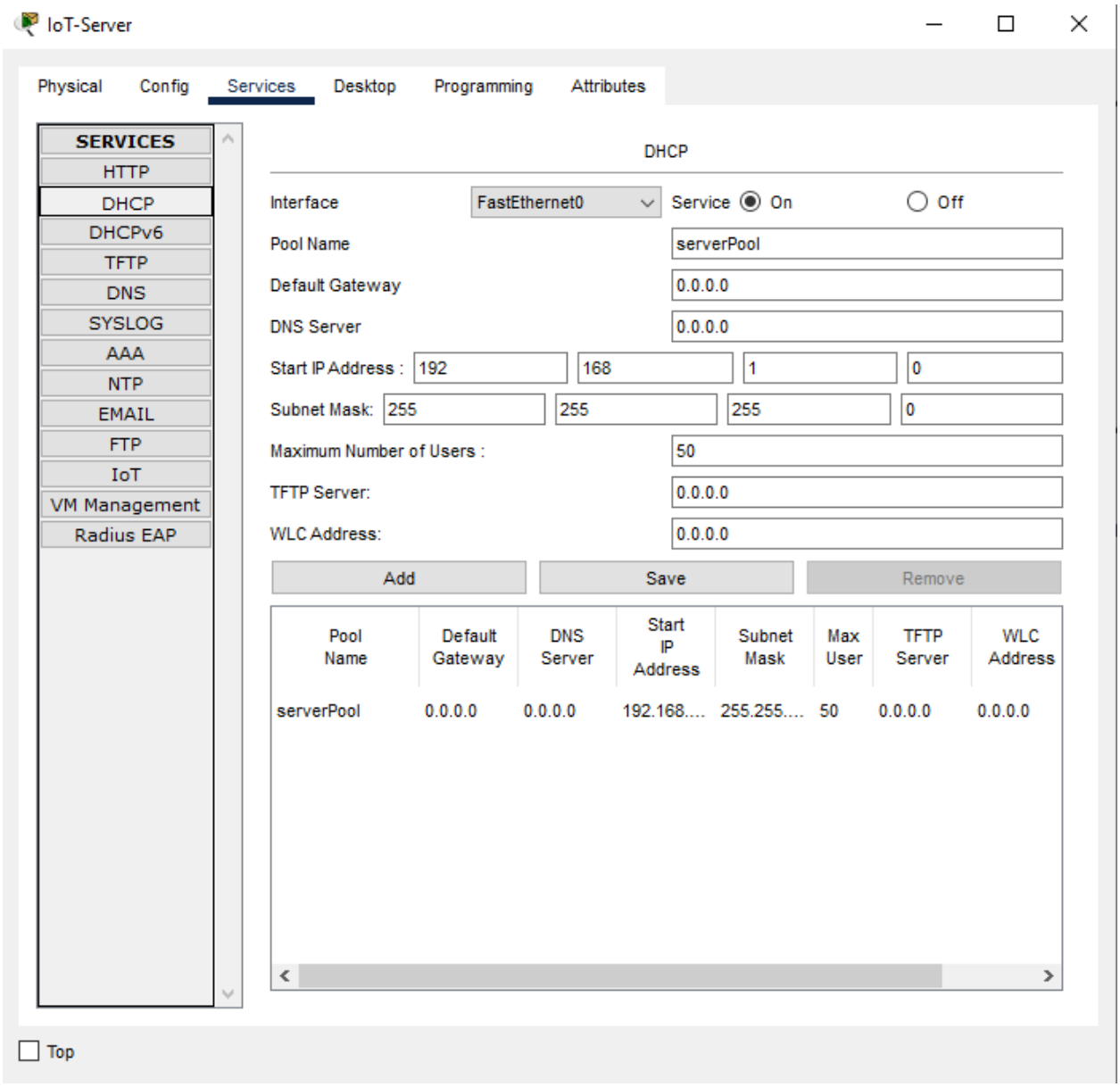

Рисунок 3.1.3 - Демонстрація налаштування DHCP на сервері

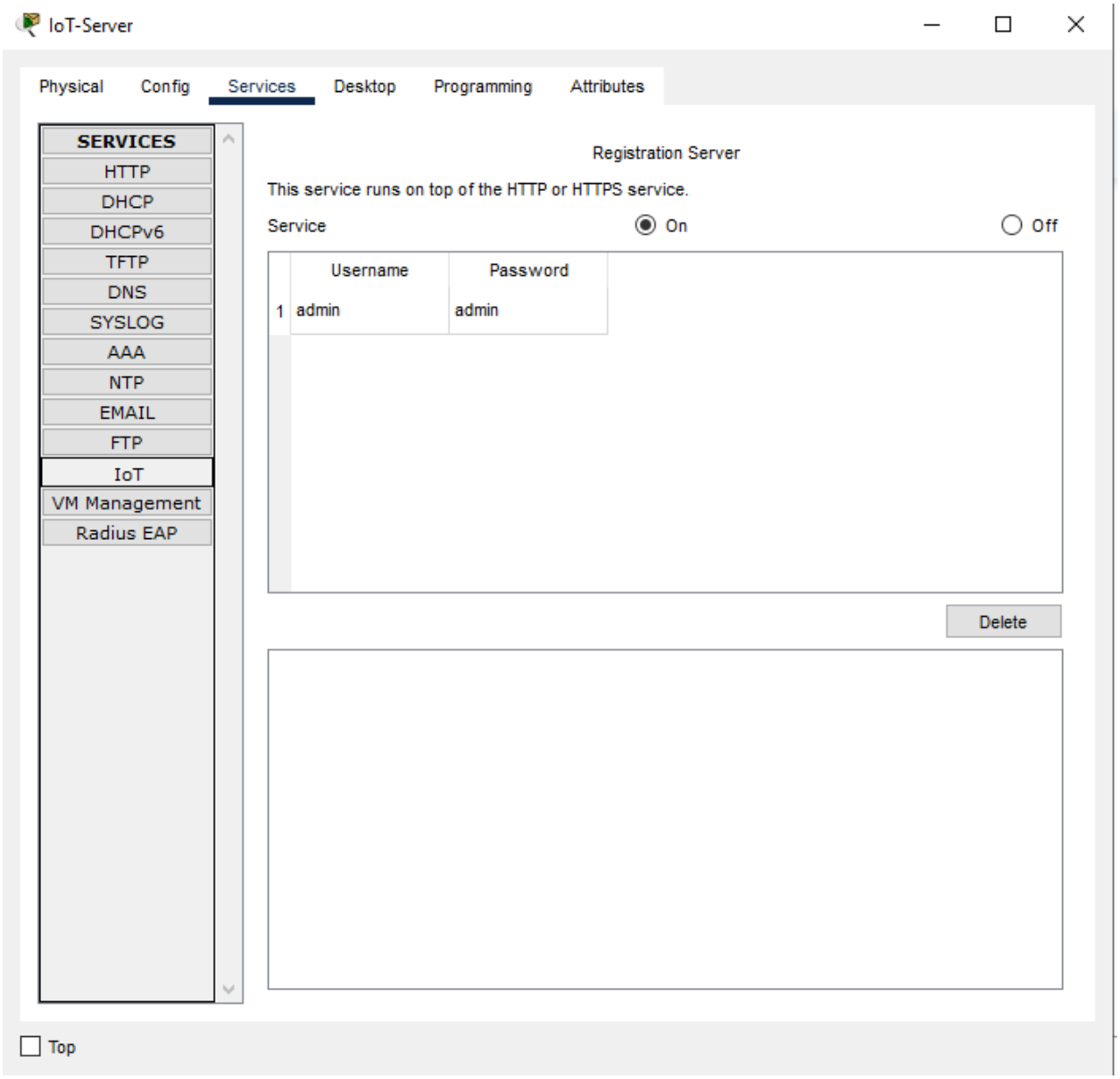

Рисунок 3.1.4 - Демонстрація налаштування IoT сервіса на сервері

Після налаштування всіх потрібних сервісів, можна починати під’єднувати пристрої в мережу, використовуючи світчі та точки доступу на рисунку 3.1.5.

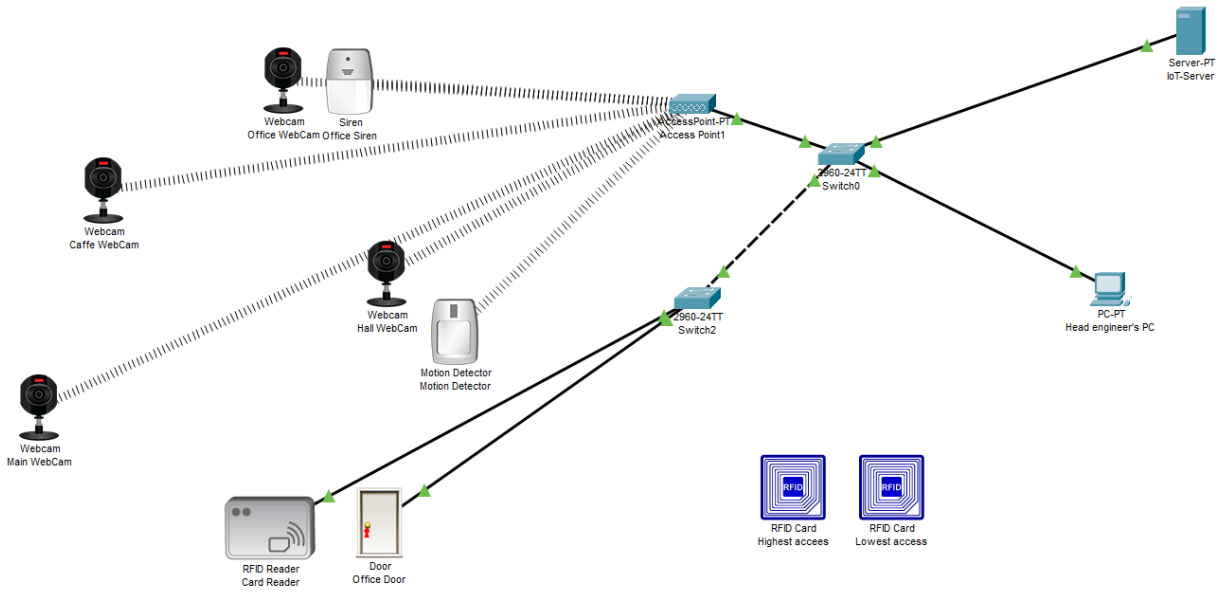

Рисунок 3.1.5 - підключення світчів та точки доступу до мережі за допомогою Copper Straight-Through (Мідна пряма) кабелем

Наступним кроком буде налаштування точки доступу для подальшої можливості підключення безпроводним способом пристроїв безпеки (Рисунок 3.1.6).

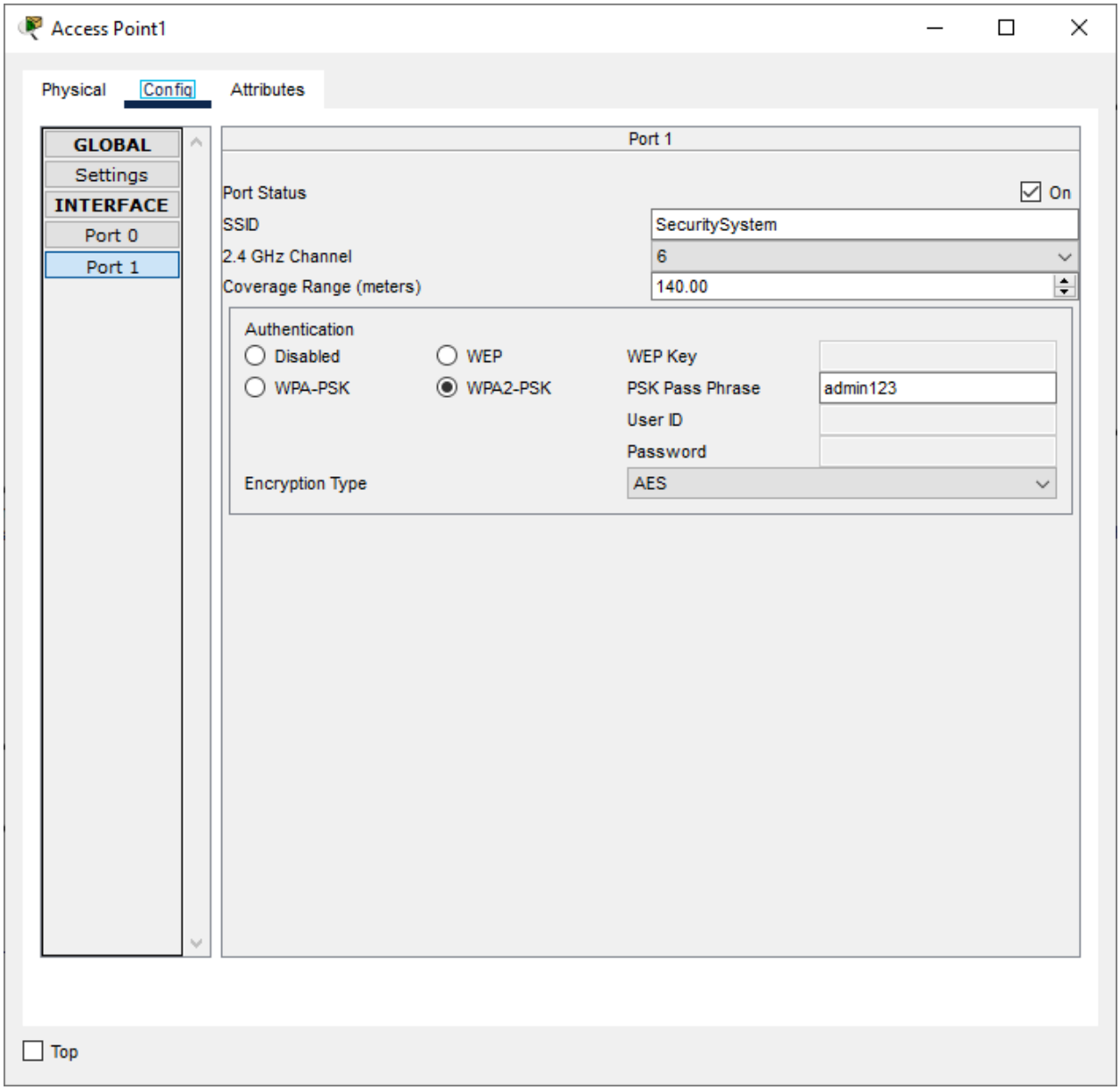

Рисунок 3.1.6 - Налаштування точки доступу (Назва мережі та тип аутентифікації)

Наступним кроком буде підключення всіх пристроїв у яких тип підключення є безпроводним (Рисунок 3.1.7).

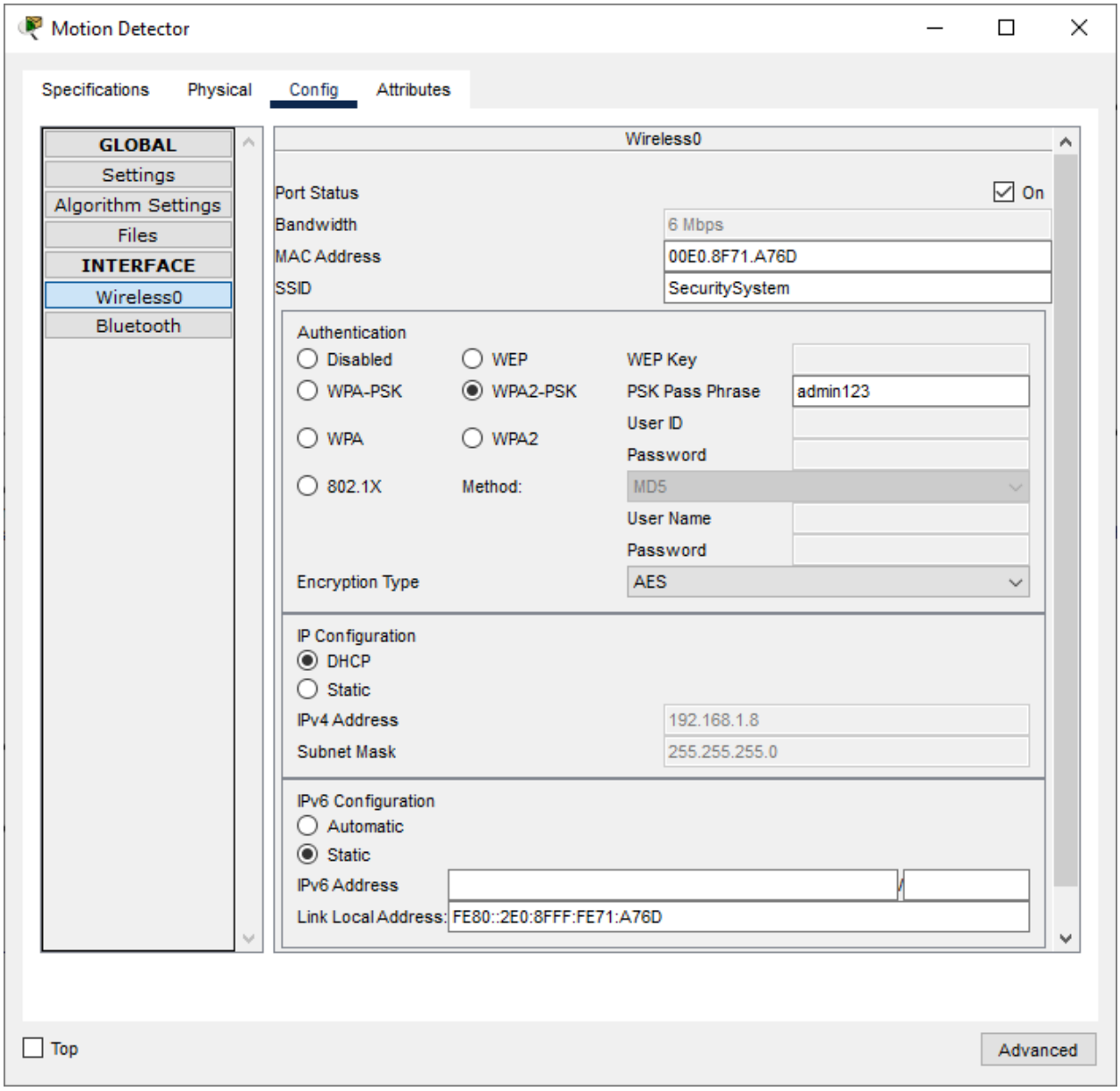

Рисунок 3.1.7 - Підключення пристрою безпроводним типом підключення

В результаті вийде така логічна топологія з підключених пристроїв до мережі на рисунку 3.1.8.

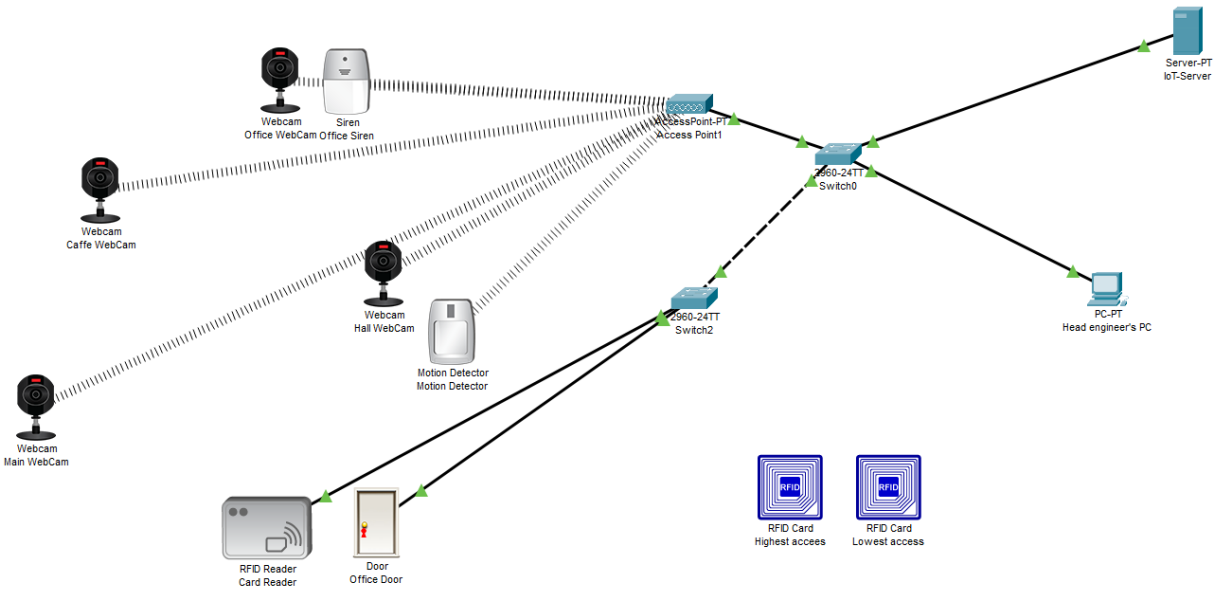

Рисунок 3.1.8 - Логічна топологія підключених пристроїв

Коли всі пристрої підключені, можемо приступати до написання правил взаємодії між пристроями IoT. Але перед цим, треба налаштувати отримання адреси пристрою в мережі за протоколом DHCP (Рисунок 3.1.9), метод підключення та адресу місцезнаходження серверу з сервісом IoT (Рисунок 3.1.10).

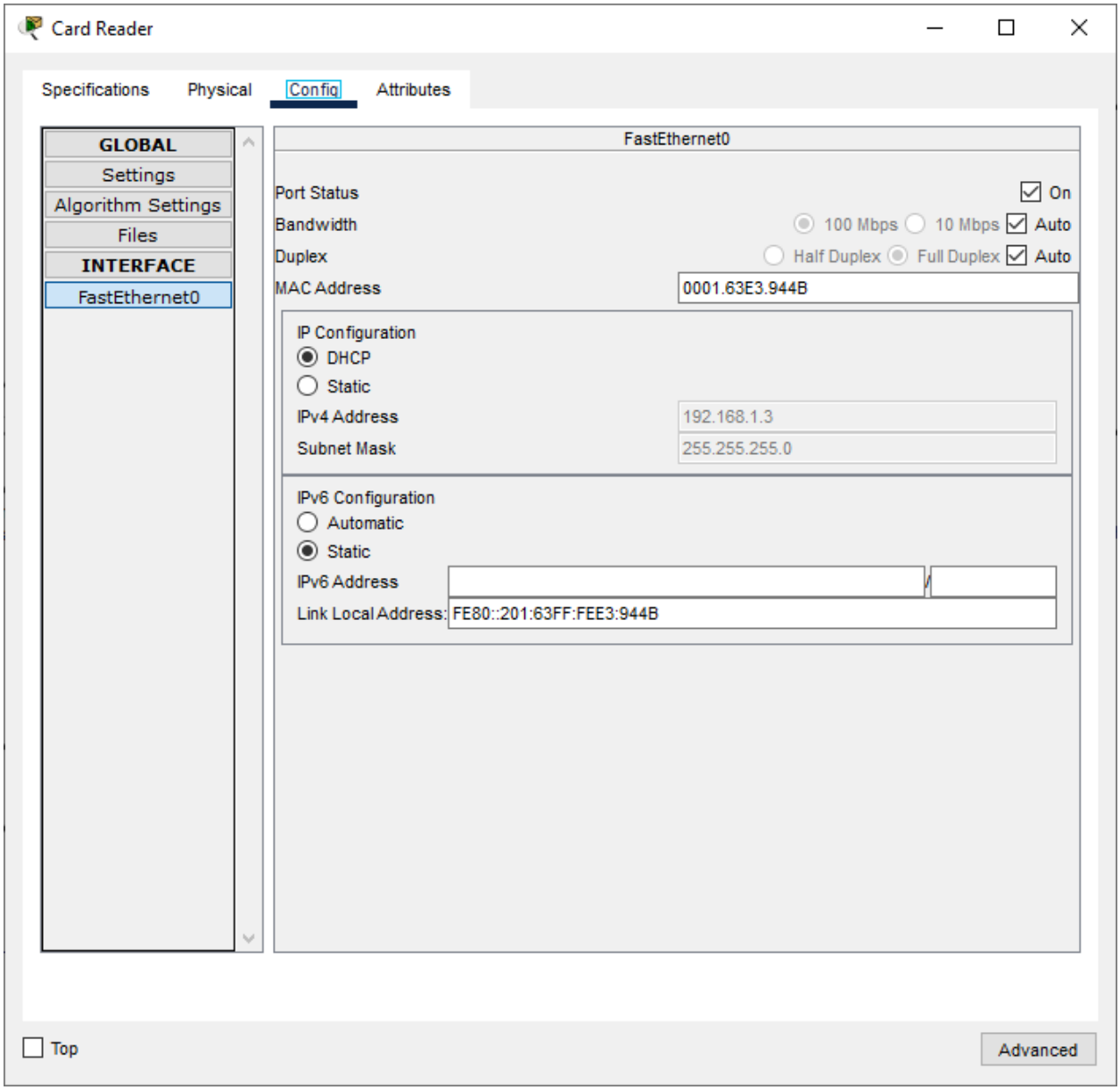

Рисунок 3.1.9 - Використання DHCP протоколу для автоматичного отримання адреси пристрою в мережі від сервера

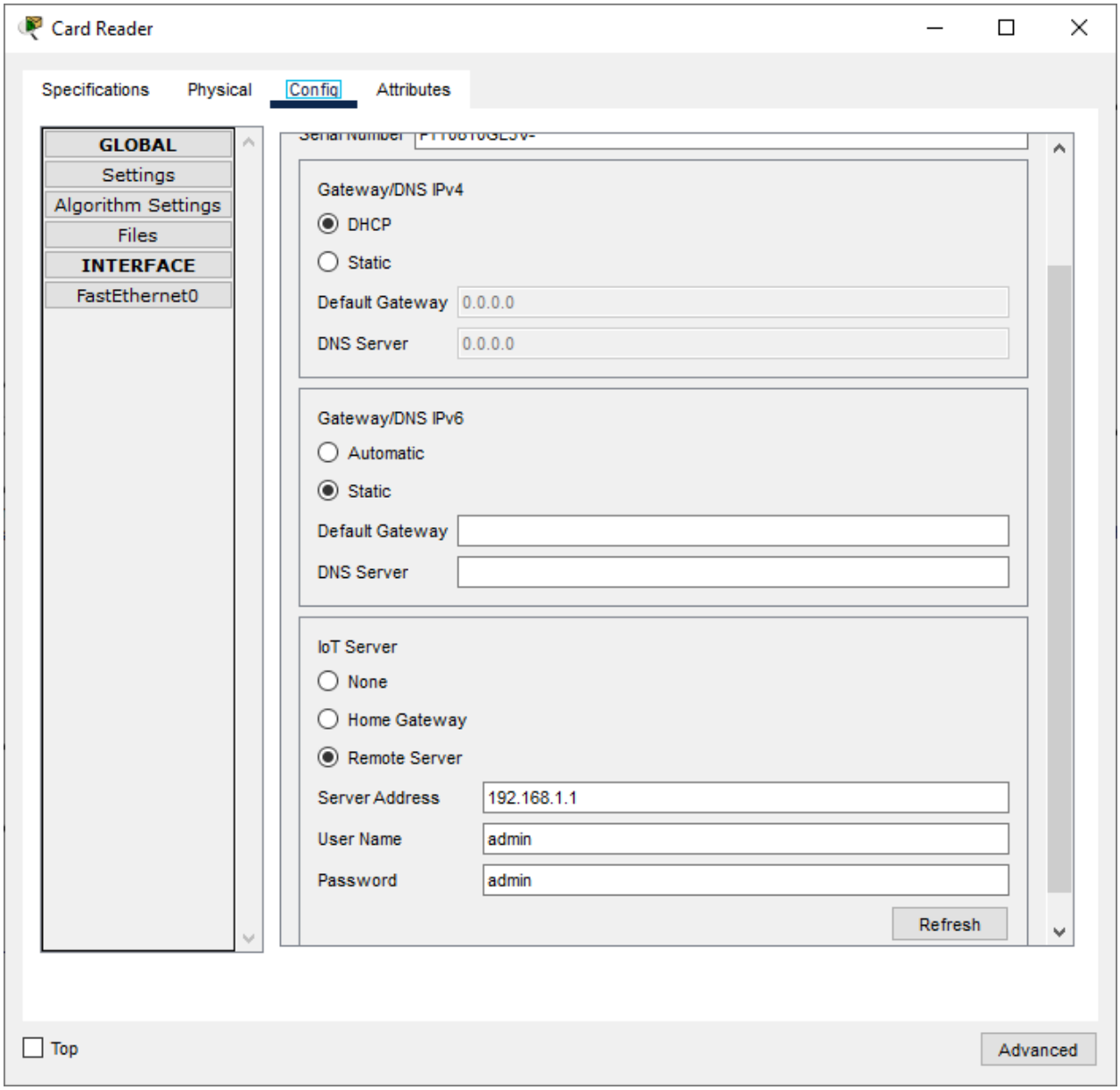

Рисунок 3.1.10 - Налаштування адреси серверу та credentials для автентифікації IoT серверу

Тепер можемо зайти на сторінку IoT-монітора через пристрій підключений до мережі (наприклад через персональний комп'ютер головного інженера) та налаштовувати взаємозв'язки між пристроями (Рисунок 3.1.11). Після входу, можемо побачити список підключений пристроїв (Рисунок 3.1.12).

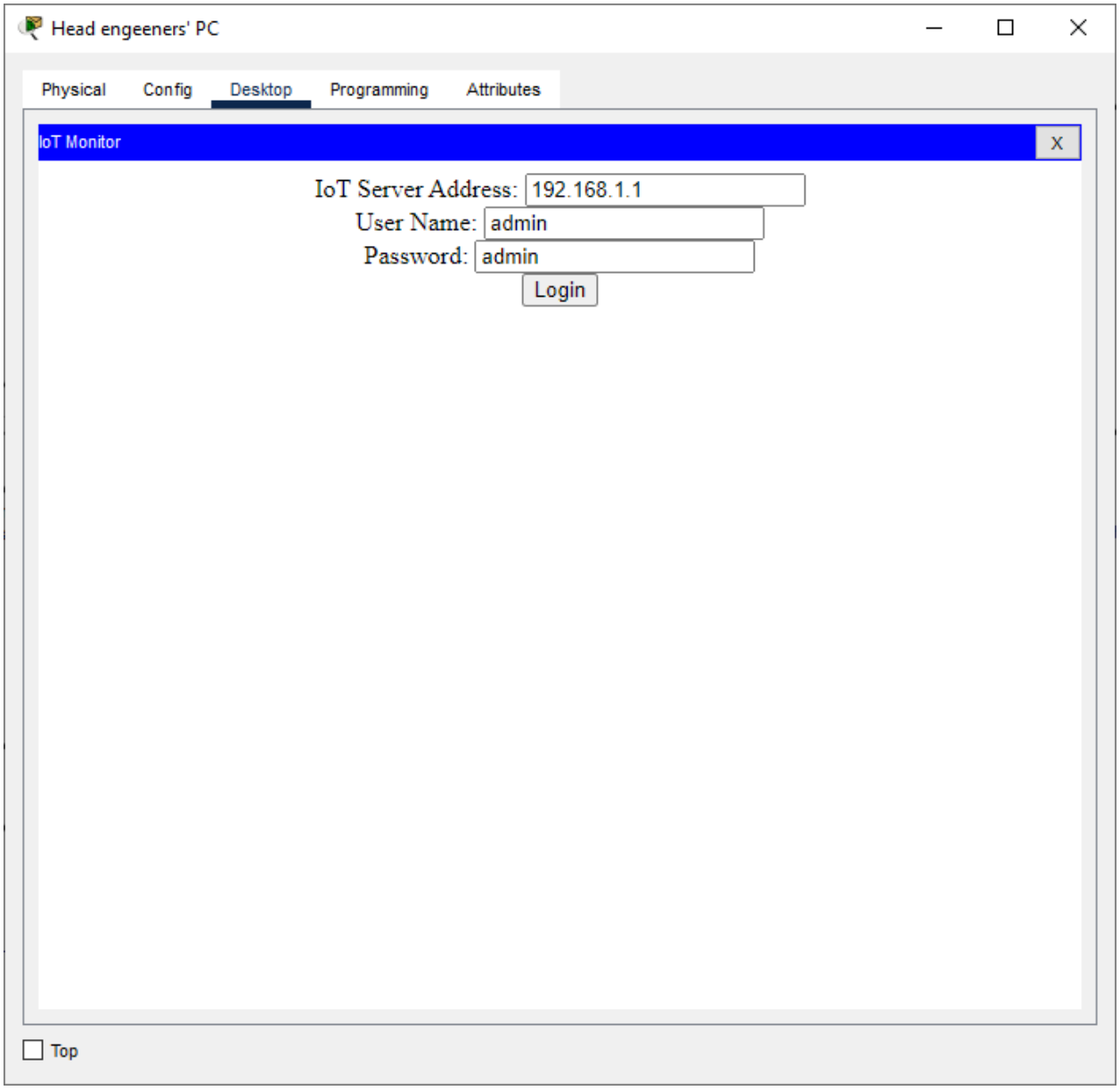

Рисунок 3.1.11 - Вхід в IoT Monitor через персональний комп’ютер головного інженера

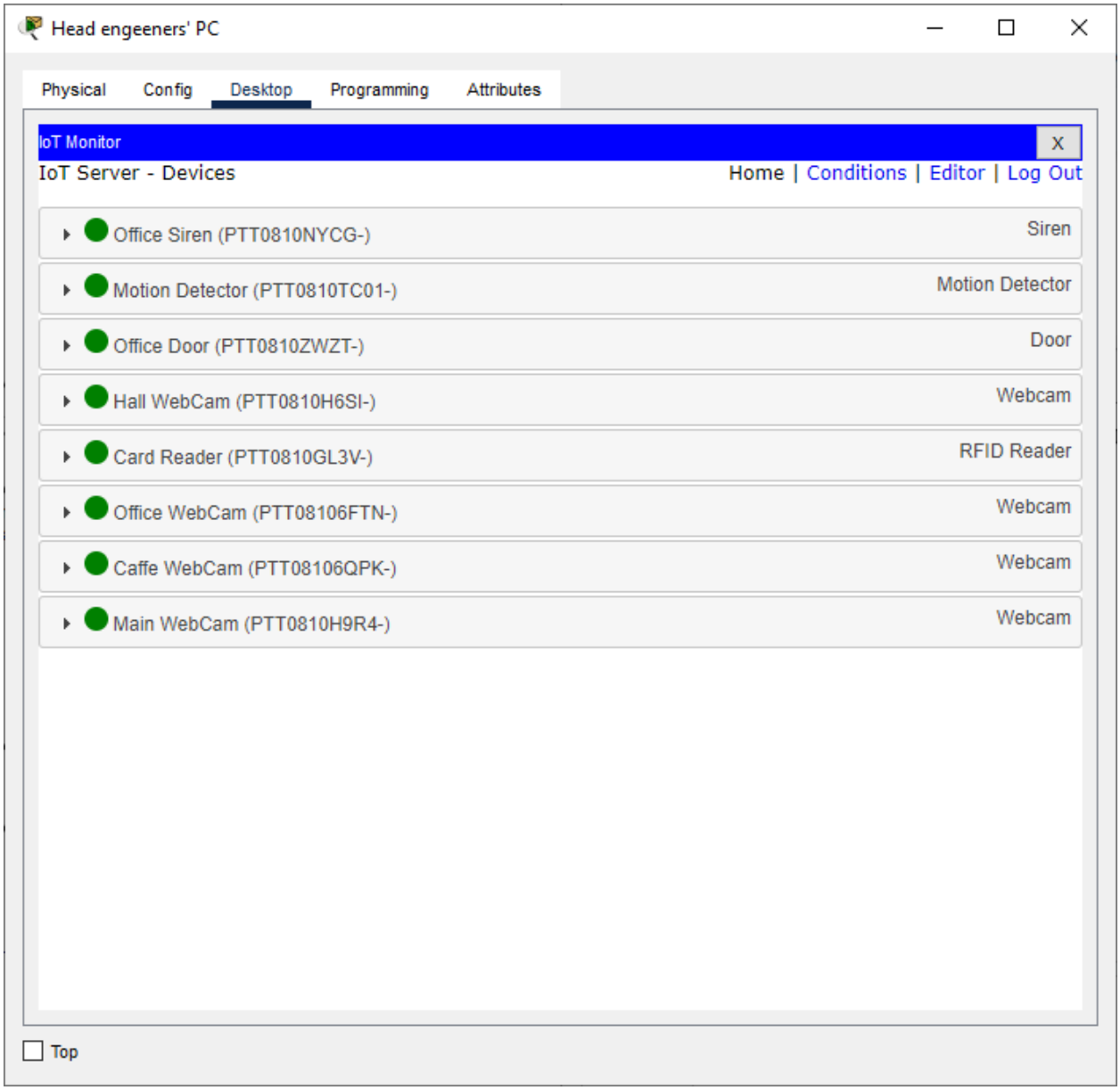

Рисунок 3.1.12 - Список підключених пристроїв в мережі

Наступним кроком буде налаштування правил поведінки підключених пристроїв в мережі через даний інтерфейс на рисунку 3.1.13.

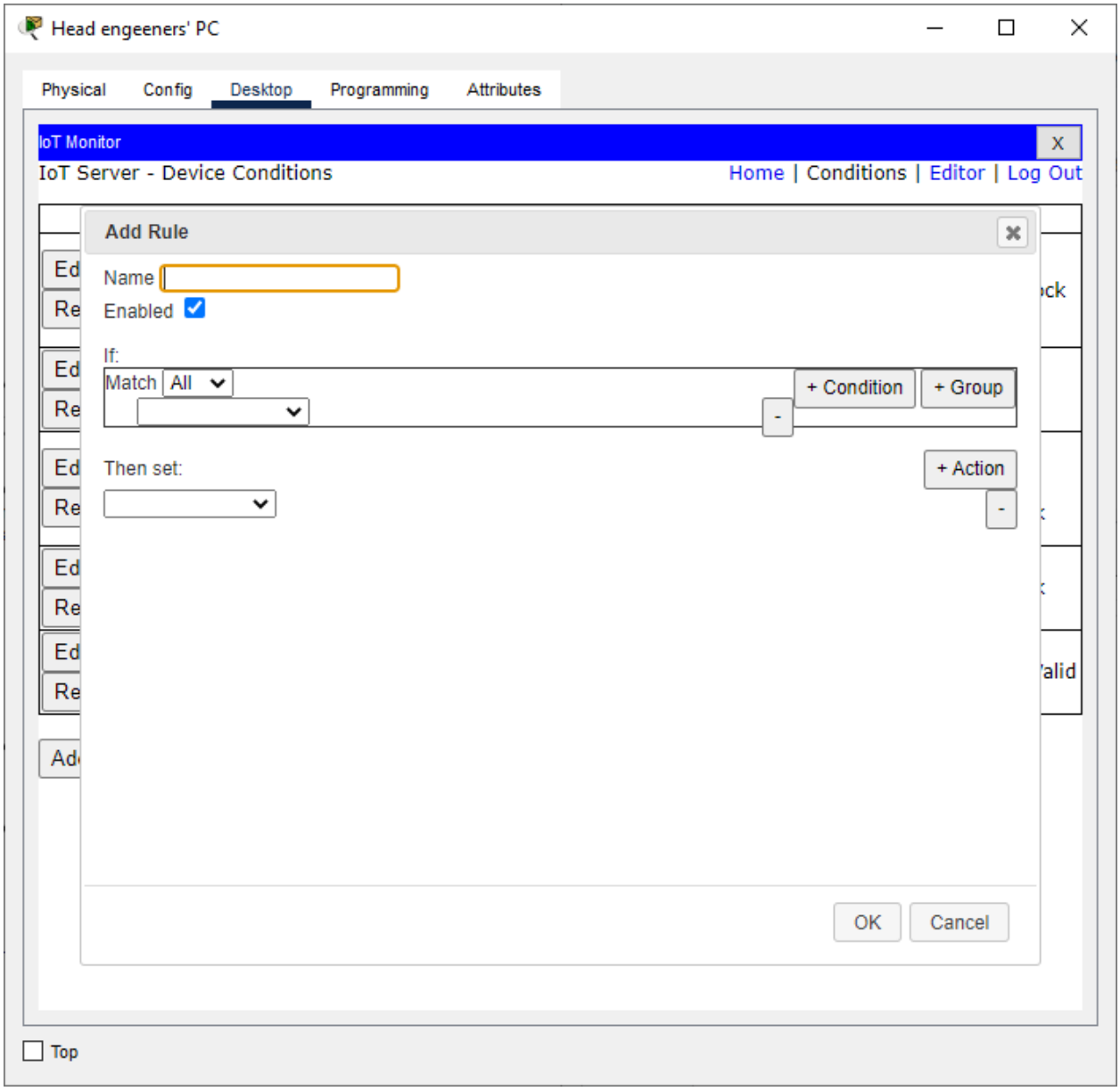

Рисунок 3.1.13 - Інтерфейс додавання нового правила

Для симуляції системи, нам потрібно створити ці правила поведінки пристроїв дані на рисунку 3.1.14.

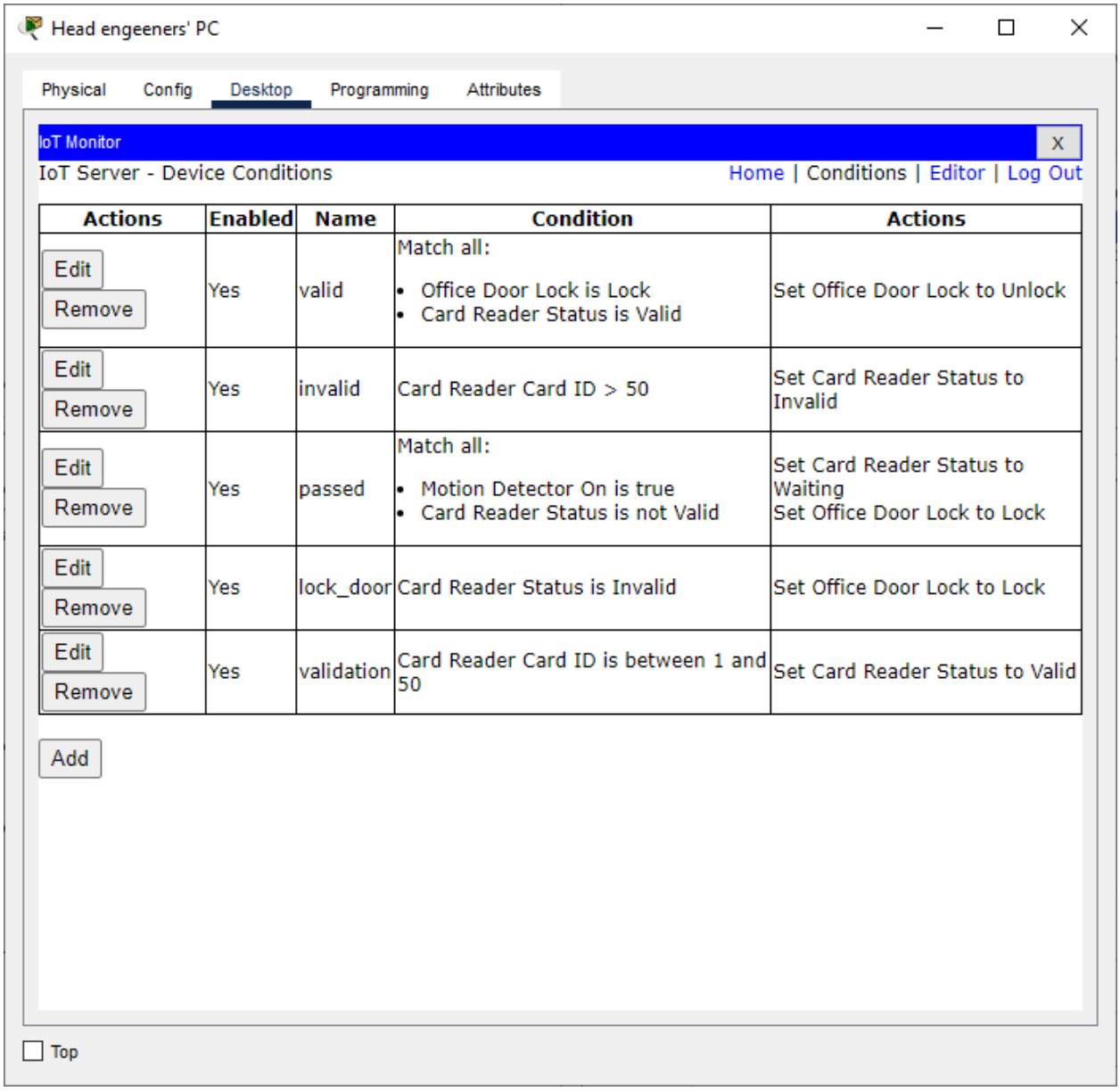

Рисунок 3.1.14 - Список правил, необхідних для симуляції системи

Настав час для тестування нашої системи. Для цього, нам треба дві картки доступу - одна з необхідним рівнем доступу, а інша - з низьким. В даній симуляції це робиться за допомогою ідентифікаторів на картках (даний шлях симуляції картки з використанням Id є ненадійним та не забезпечує достатнього рівня безпеки, але для симуляції системи в навчальних цілях - можливий варіант).

Для тестування системи піднесемо картку з недостатнім рівнем доступу до картридера та отримуємо результат на рисунку 3.1.15.

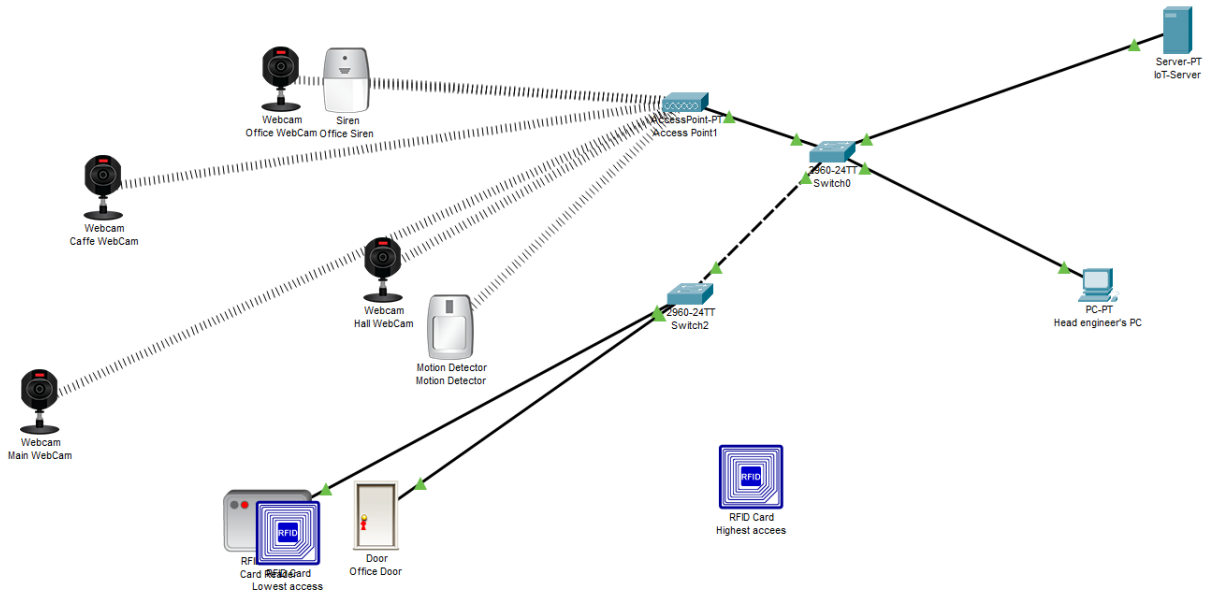

Рисунок 3.1.15 - Використання картки з недостатнім рівнем доступу

Як видно з рисунку 3.1.15 - не можна отримати доступ та відкрити електронні двері. Для розблокування дверей нам необхідна картка з достатнім рівнем доступу. Піднесемо картку з необхідним рівнем та отримуємо результат на рисунку 3.1.16.

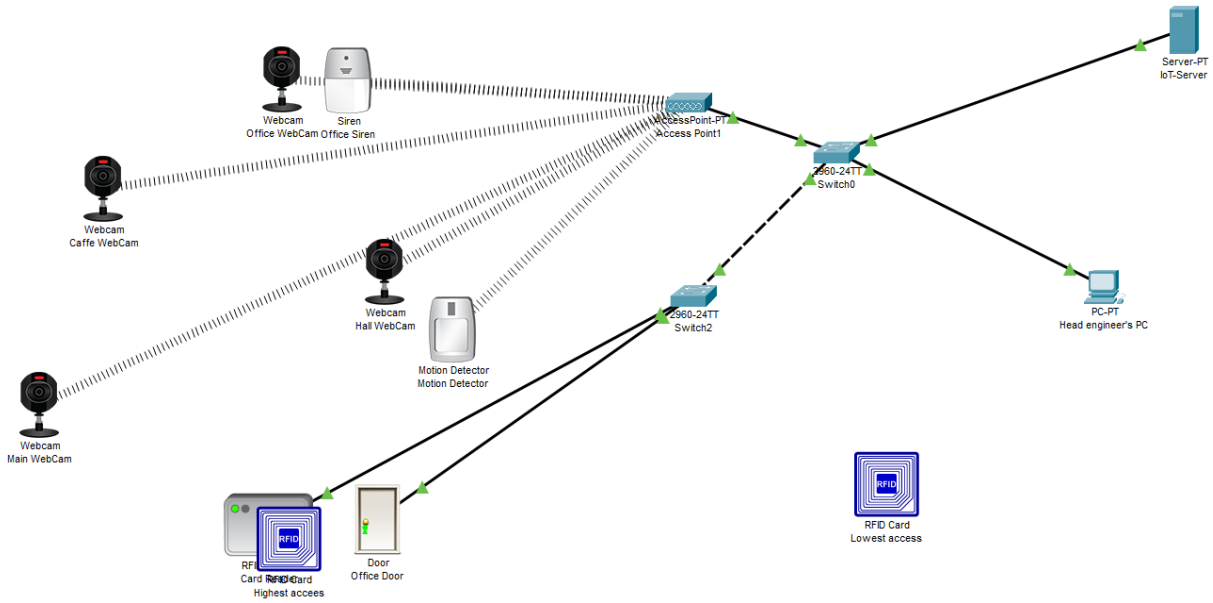

Рисунок 3.1.16 - Використання картки з достатнім рівнем доступу

Тепер, коли доступна картка з достатнім рівнем доступу, можна вільно відкривати електронні двері та пересуватися по офісу. Після використання картки, ми маємо змогу відкрити двері один раз та після закриття вони автоматично блокуються. Або ж, як альтернатива, після дверей стоїть датчик руху, який при спрацюванні блокує двері.

ВИСНОВКИ

Основний висновок на основі проведеного аналізу та дослідження впровадження рішень Інтернету речей (IoT) в системи контролю та управління доступом полягає в тому, що це відкриває нові можливості для підвищення безпеки, ефективності та зручності. Завдяки IoT, створюються інтелектуальні мережі, які дозволяють автоматизувати рутинні процеси, забезпечують гнучкість, масштабованість та віддалене керування. Ці рішення сприяють збереженню часу та зусиль, а також підвищують рівень безпеки та контролю в різних сферах діяльності, включаючи підприємства, комерційні приміщення, житлові комплекси та офіси.

Аналіз показав, що впровадження IoT в системи контролю доступу дозволяє використовувати різноманітні пристрої, такі як карт-рідери, біометричні сканери, сенсори руху та інші "розумні" пристрої, що підключаються до мережі Інтернет. Це забезпечує точність, швидкість та безпеку у системі контролю доступу. Крім того, існує можливість віддаленого керування та моніторингу, що дозволяє користувачам керувати доступом до приміщень, стежити за журналами входів-виходів, налаштовувати права доступу та отримувати повідомлення про неправильні спроби або незвичайну активність. Це сприяє зручності та оперативній реакції на потенційні загрози.

Ще однією перевагою використання IoT в системах контролю доступу є їх гнучкість та легка масштабованість. Системи IoT можуть бути легко розгорнуті та розширені в залежності від потреб організації або об'єкту, додавання нових пристроїв до мережі не потребує значних зусиль або затрат. Це дозволяє підлаштовувати систему під зростаючі вимоги та змінні потреби.

Недавні технологічні розробки в галузі IoT дозволяють впроваджувати аналітику та інтелектуальні алгоритми в системи контролю доступу. Це дає можливість виявляти незвичайну активність, розпізнавати образи, ідентифікувати

особу за мімікою або голосом, а також прогнозувати поведінку та аналізувати дані для покращення ефективності та безпеки.

Таким чином, впровадження IoT в системи контролю та управління доступом є перспективним рішенням, що принесе вагомі переваги. Воно розширює можливості традиційних систем контролю доступу, забезпечуючи більшу ефективність, безпеку та зручність. З використанням IoT створюються інтелектуальні мережі, які допомагають автоматизувати рутинні процеси, реагувати оперативно на потенційні загрози та пристосовуватись до змінних потреб організацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стаття на тему “What is the Internet of Things, or IoT” URL: https://www.iotforall.com/what-is-internet-of-things (електронний ресурс)
2. Стаття на тему “The hidden risks of connected devices” was written by Rob Williams URL:https://www.iotworldtoday.com/security/security-the-hidden-risks-of-connected-devices (електронний ресурс)
3. Стаття на тему “IoT-protocols” was written by Dimitris Paraskevopoulos URL:https://iot-analytics.com/iot-protocols (електронний ресурс)
4. Стаття на тему “Переваги систем контролю доступом” URL: https://www.iotforall.com/smart-locks-and-access-control-systems-combine-for-better-buildings (електронний ресурс)
5. Стаття на тему “Топ використання IoT” URL: https://iot-analytics.com/top-10-iot-use-cases (електронний ресурс)
6. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things, Pearson Education, 2017, P. 576 (книга, 4 автори)
7. Сайт з розбіром сучасних систем безпеки URL: https://www.securityinfowatch.com/ (електронний ресурс)
8. Ресурс, що пропонує статті та новини про застосування IoT в різних сферах, включаючи системи контролю та управління доступом URL: https://www.iotforall.com/ (електронний ресурс)
9. Сайт, який надає інсайти, статті та аналітику про розвиток IoT і його вплив на системи контролю та управління доступом URL: https://www.techtarget.com/iotagenda/ (електронний ресурс)
10. Ресурс, де можна знайти новини, статті та практичні поради про використання IoT в системах контролю та управління доступом URL: www.iotworldtoday.com (електронний ресурс)

11. Сайт, що спеціалізується на аналітиці та дослідженнях IoT, включаючи аналіз застосування IoT у системах контролю доступом URL: https://iot-analytics.com/ (електронний ресурс)
12. Ресурс, що пропонує технічні статті та новини про системи контролю та автоматизацію, включаючи інформацію про IoT у контексті контролю доступу URL: https://www.controleng.com/ (електронний ресурс)
13. Сайт, який охоплює новини та статті про системи безпеки, включаючи інформацію про ролі IoT у системах контролю та управління доступом URL: https://www.securitysystemsnews.com/ (електронний ресурс)
14. Ресурс, що пропонує статті та інформацію про системи контролю доступом та їх інтеграцію з іншими системами безпеки URL: https://www.asmag.com/ (електронний ресурс)
15. Сайт, де можна знайти новини та статті про рішення безпеки, включаючи теми з систем контролю та управління доступом, які пов'язані з IoT URL: https://www.discoverisc.com/global/en-us.html (електронний ресурс)
16. Видання, яке пропонує новини та статті про технології, включаючи Інтернет речей та системи контролю доступу URL: https://www.computerworld.com/ (електронний ресурс)
17. Науковий журнал, що публікує дослідження та статті з розподілених мереж сенсорів, включаючи їх застосування в системах контролю та управління доступом URL: https://journals.sagepub.com/home/dsn (електронний ресурс)
18. Альянс, що сприяє розвитку технологій смарт-карт та їх застосування, включаючи системи контролю доступу та інтеграцію з IoT URL: https://www.securetechalliance.org/ (електронний ресурс)