M. M. Zaporozhchenko, T. M. Dzyuba

SOCIAL ENGINEERING ATTACKS LIFE CYCLE AND TYPES

Today, social engineering attacks are one of the most common methods for hackers to hack computer networks and information systems of organizations, steal credentials and other confidential information of users, and commit various cybercrimes. Socio-engineering attacks pose a particular threat to companies with large numbers of employees. Without proper training and education of staff, an attack on an employee who is not related to information security is more likely to be successful, but even such an employee may not be the main cause of a company's information security incident, but become one of the links in the attack chain. which the attacker created to achieve his ultimate goal. Given this, the need to raise awareness about socio-engineering attacks, namely how they are implemented and what types of them exist. This article describes the life cycle of social engineering attacks and the main methods that are used by attackers to implement such attacks. Company employees should be familiar with the signs and examples of various types of social engineering attacks in practice, the principles and rules for working with information, as well as the responsibility for violating these rules. To ensure data security, regulations and instructions should be created and communicated to the personnel, which should clearly spell out the rules for storing, processing, distributing and transferring information to third parties. Raising the awareness of the company's employees about the types of social engineering attacks will reduce the number of incidents implemented as a result of their occurrence.

Keywords: social engineering; information security; cybersecurity; attack life cycle; phishing.

УДК 004.738.5+681.5

DOI: 10.31673/2412-9070.2021.042025

М. О. МАКАРЦЕВ, магістр;
А. М. ТУШИЧ, доктор філософії, доцент;
І. В. ЗАМРІЙ, канд. техн. наук, доцент;
Л. Т. АЛЕКСІНА, ст. викладач,
Державний університет телекомунікацій, Київ

ПРОБЛЕМИ, ТРУДНОЩІ і МОЖЛИВОСТІ IoT ТА ХМАРНИХ ОБЧИСЛЕНЬ

З розвитком Індустріального Інтернету речей (IIoT) спостерігається постійне зростання обсягу інформації. Проте недоцільно зберігати всі необроблені дані в пристроях IIoT, оскільки енергія кінцевих пристроїв не є невичерпною, а додаткові приміщення жорстко обмежені. Мережі IoT розширюють можливості присвоєного асортименту інформації та розподіленого сховища, незалежно від штучної природи IoT. Існує низка невизначених гарантій для проблем IoT та інтеграції у хмару. Хмарні обчислення є високоефективними, зберігання стає дедалі актуальнішим, і деякі групи зараз пересилають свої дані з власних записів у центри постачальників хмарних обчислень. Інтенсивні програми IoT для робочих навантажень і даних можуть спричинити труднощі під час використання розподілених обчислювальних апаратів. У статті досліджено IoT та хмарні обчислення, а також розглянуто сумісні з хмарою проблеми та обчислювальні техніки для сприяння стабільному переходу програм IoT до хмари.

Ключові слова: Інтернет речей; IoT; хмарні обчислення; безпека; IoT-хмара.

ВСТУП

Публічна хмара та IoT — це дві окремі, але міцні системи, інтегровані, щоб стати важливою частиною майбутнього інтернету. Ці інтеграції розглядаються як величезний диверсійний процес із великими перевагами в майбутньому. Значна зміна вноситься в IoT та хмару. Для розв'язання проблем, що постали в процесі аналізу інтеграції IoT з хмарними обчисленнями, нам знадобиться відповісти на такі запитання:

• Яка потреба в інтеграції IoT з хмарними обчисленнями?

• Чи спричинить інтеграція IoT з хмарою будь-які проблеми?

Мета статті полягає у вивченні можливостей та проблем застосування IoT та хмарних обчислень, вирішенні проблем, сумісних із хмарою, та обчислювальних технік для сприяння стабільному переходу програм IoT до хмари.

ОСНОВНА ЧАСТИНА

Останніми роками хмарні обчислення та IoT дуже швидко поширились у всьому світі. Характеристики, які вони демонструють, можуть бути доволі корисними в поєднанні. Кожен із них справді особливий і важливий один для одного. Оскільки IoT отримує допомогу від хмарного сховища та обчислювальних можливостей, дослідники запланували низку програм, що стосуються координації хмари та Інтернету речей, для розроблення та нагромадження даних. Архітектуру Cloud-IoT (Cloud and IoT), в якій прикладний, мережний та сенсорний рівні знань взаємозв'язані, зображено на рис. 1.

Об'єкти, здатні зчитувати та збирати дані через різні системи IoT, розміщують через протоколи візуалізації IoT. Для полегшення оброблення ці знання можуть упорядковуватися в хмарі. Прикладний рівень може сприймати дані навколиш-

Рис. 1. Архітектура Cloud-IoT

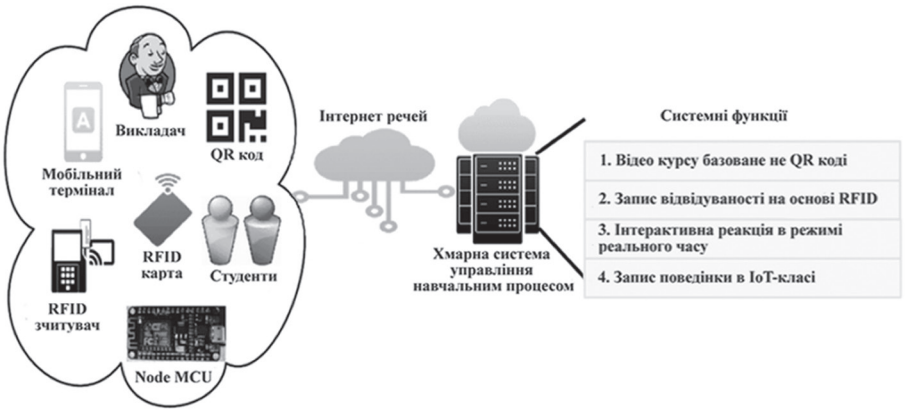

Рис. 2. Середовище Cloud-IoT

нього середовища та одночасно надсилати запити до хмари для оброблення та отримання результатів інформації про давачі. Крім того, для додаткового оброблення потрібно ще раз розміщувати інформацію в IoT та інших об'єктах IoT, а також отримані з сенсорного рівня дані та їх аналіз.

Для взаємодії між пристроями в інтернеті застосовується RESTful з вебсерверами та протоколом простого доступу до об'єктів (SOAP). SOAP Web Services працює зі спільним використанням XML, але більшість WSS співдіє з протоколом HTTP, необхідним для ресурсів та комп'ютерів із лімітованим енергоспоживанням (рис. 2). Протокол програм обмеженого застосування (CoAP) потребує використання засобів RESTful на комп'ютерах із мінімальними ресурсами. Для безпроводового зв'язку між пристроями з обмеженим доступом до ресурсів CoAP використовує протокол UDP замість TCP, який доволі поширений у HTTP.

Задачі хмарного IoT

Середнім шаром між об'єктами та програмами є хмарне сховище, яке приховує нюанси та функції. Як відомо, IoT — це мережа пов'язаних об'єктів із різними програмами, які беруть участь у цих об'єктах. Проблеми унікальні для кожної програми, але вони зазвичай належать до подібної категорії. Щоб розв'язати ці проблеми, потрібно зосередитись переважно на безпеці та оцінити наслідки нових методів. Після інтеграції хмари та IoT постійно виникають занепокоєння щодо недовіри провайдера хмари та розуміння фізичного розташування даних, що передаються в хмару за допомогою різних протоколів IoT. Існує кілька проблем щодо системи зберігання даних у хмарній службі, яка містить кілька орендарів. Багато інформації про споживача розміщується в одному об'єкті, що може зашкодити конфіденційності та призвести до витоку конфіденційної інформації. Сьогодні через недовіру до постачальника хмарних послуг ця форма вразливості вважається внутрішньою загрозою і є однією з найбільш непередбачуваних проблем IT-галузі. Розглянемо деякі критичні проблеми хмарного IoT.

• ***Захист.*** Дані з Інтернету речей розміщено в хмару для оброблення і вилучення. Цей процес включає в себе шифрування даних, що відправляються або зберігаються в хмарних репозиторіях, та безпеку даних під час доступу і використання хмари. Ступінь нестачі інформації про хмарні обчислення такий, що власники даних не розуміють фізичне становище своїх персональних даних. Сьогодні дані пов'язані з усім, що нас оточує, тому безпека даних у парадигмі Cloud-IoT є головною темою.

• ***Зберігання та обчислювальна продуктивність.*** Плани, які зосереджено на використанні хмарних пристроїв IoT, потребують високого ступеня вимог до продуктивності. За будь-яких умов ці специфікації важко задовольнити, оскільки хмарні пристрої Інтернету речей перебувають у русі для багатьох додатків.

• ***Надійність.*** Пристрої IoT залежать від постачальників хмарних послуг для критичних за часом додатків, а отже, ефект буде безпосередньо позначатися на результаті роботи програми. Наприклад, в автомобілях, хірургічних інструментах або у сфері безпеки.

• ***Зберігання великих даних.*** Майже 75,5 млрд пристроїв IoT буде введено в експлуатацію до 2025 року, і цей обсяг може стати значною перешкодою для постачальників хмарних послуг — мати швидкий та безпечний доступ до даних.

• ***Технічне обслуговування.*** Для задоволення вимог чималої (75,5 млрд) кількості пристроїв IoT потрібно мати надзвичайно ефективні методи та плани для відстеження й керування захистом та ефективністю в хмарному середовищі.

• ***Периферійні обчислення.*** Обмеження затримки, обмеження мобільності і реалізації IoT з географічним розподілом вимагають негайної відповіді хмари. Тому периферійні обчислення — це компроміс між класичними та хмарними обчисленнями. Хоч ми і наближаємося до їх реалізацій, проте залишаються труднощі в запровадженні, оскільки їм потрібне усвідомлення позиції.

• ***Пристрої IoT, що підтримуються користувачем.*** Очікується, що в таких реалізаціях IoT користувачі послуговуватимуться деталями і перевагами, які будуть компенсовані за їх участь в обміні. Це важлива проблема, оскільки починають діяти соціальні фактори, коли споживач зі свого боку робить свій внесок.

• ***Взаємодія з пристроями.*** Хмарні IoT системи часто потребують отримання даних із широкого кола пристроїв, які підлягають обробленню та впровадженню. У цій ситуації такі специфікації, як простір для зберігання даних та хмарні обчислювальні можливості, можуть стати жорсткими.

Огляд літератури

Стосовно IoT та хмарних обчислень, то вони перебувають на двох різних «континентах». Однак їх властивості поєднуються, саме тому конвергенція вигідна обом.

Mohiuddin Irfan та ін. [1] обговорювали проблеми, пов'язані з блоками зберігання даних у центрах оброблення даних. Було досліджено спеціальний метод класифікації для забезпечення однакового розподілу навантаження, а також ключовий внесок у підхід до міграції на основі віртуальних машин (VM). Міграцію віртуальних машин призначено для консолідації віртуальних машин залежно від навантаження, зменшення використання ресурсів та заохочення «зелених» обчислень. Отже, було запропоновано метод під'єднання віртуальних машин з урахуванням навантаження (WAVMCM). Автори статті також перевіряли цей метод, порівнюючи його із залежним від штучного інтелекту імовірнісним методом, включно з модельованою нормалізацією, генетичним алгоритмом та експериментом для порівняння швидкості роумінгу між секціями. Експерименти показали, що WAVMCM зменшує кількість працюючих серверів на 9%, заощаджуючи 15% споживання електроенергії центральним процесором, ніж підходи, засновані на генетичних алгоритмах.

Zhang Wei-Zhe та ін. [2] рекомендували спільну стратегію балансування навантаження та розвантаження мобільних обчислень на кінцевих пристроях (MEC), додавши новий рівень безпеки для зменшення можливих її проблем. Далі пропонується алгоритм балансування навантаження для ефективного розподілу користувачів мобільних пристроїв sBS (MDU). Крім того, нова розширена криптографічна технологія стандарту шифрування (AES) подана як захисний рівень для захисту вразливості даних під час передавання за допомогою шифрування та дешифрування сигналу на основі електрокардіограми (ЕКГ). Оптимізована модель для балансу навантаження, вивантаження вимірювань та захисту часто розглядається як проблема зменшення часу та енергетичних потреб системи. Детальні експериментальні результати показують, що порівняно з виконанням на місці споживання машини з додатковим рівнем безпеки та без нього заощадить майже відповідно 68,2 та 72,4%.

У статті Riad Khaled та ін. [3] запропоновано програмне забезпечення багатовимірного контролю доступу (MD-AC) для динамічного дозволу та видалення користувачів у хмарі за допомогою різних повноважень. Результати експерименту демонструють, що MD-AC визначатиме запити на доступ протягом розумного та відповідного періоду. Середній час шифрування та дешифрування становить відповідно 18 та 10 мс, незважаючи на дуже складні лабораторні умови та багаторазові транзакції. Запропонована схема також перевірена та протиставлена сучасним схемам останніх років. Результати показують, що запропонований режим проти численних відомих атак швидкий і стабільний. Крім того, MD-AC можна використовувати для захисту конфіденційності служб IoT у хмарному світі.

Anuradha та ін. [4] зосередили свою увагу на забезпеченні основи для підвищення поточного успіху галузі охорони здоров'я на міжнародному рівні. Звичайні медичні обмеження можна вирішити,

оскільки всі медичні записи мають зберігатися в хмарі. Для гарантування безпеки та конфіденційності онкохворих шифрування здійснюється за допомогою алгоритму AES. Акцент робиться на зручному керуванні даними про здоров'я людей, які перебувають далеко від рідного міста, оскільки необхідна терапія захворюваності на рак розміщується в хмарі. Час, відведений для виконання місії, зменшується на віртуальних машинах з 400 до 160. CloudSim пропонує модульну структуру моделювання для відображення та повторення результатів.

Ali Babar та ін. [5] запропонували проєкт добровільних обчислень туману (VSFC). Завдяки взаємодії цих двох сучасних розподілених обчислювальних сфер, можна було б скоротити затримки передавання хмарних обчислень, одночасно зменшуючи споживання енергії та потребу у використанні мережі. Для цього інструментарій iFogSim підтримує ширший спектр сценаріїв. Обчислення меж демонструють, що VSFC переважає звичайні FC-хмарні калькулятори, зменшуючи обмеження часу на 47,5; 93 та 92% за нормальних та екстремальних навантажень.

Wang Mingzhe та ін. [6] пропонують алгоритм оптимізації доступу до даних IoT у хмарних обчисленнях. У статті описано підвищену стабільність передавання даних через безпроводову мережу, що покращує технічну допомогу в обробленні та керуванні даними. Модель імітує експериментальні результати і буде запущена в OPNET Modeler. Крім того, експериментальні результати показують, що оптимізовані дані Інтернету речей більш ефективні щодо швидкості передавання, зайнятості ресурсів машини та часу відгуку. Водночас оптимізована продуктивність передавання IoT становить 99%, тоді як середня оцінка стійкості до відмов оптимізованих алгоритмів не більш як 96%.

Fuentes Henry та ін. [7] розглядають алгоритм виявлення витоків, заснований на правилах, історичному контексті та позиції користувача, які можуть визначити десять різних форм приймання, зокрема нормальний, низький, екстремальний та аномальний. Для збору даних використовується розумний лічильник, який потім надсилається на локальний сервер для аналізу й аналізований відправляється в хмару для перегляду алгоритмів в інтернеті. Здобуті дані показують, що алгоритм має 100%-кову точність, пам'ять, влучність та оцінку f1 для виявлення витоків, тобто набагато краще, ніж інші методи, і має похибку в 4,63% під час розрахунку використання води.

Abdel-Basset та ін. [8] запропонували новий пристрій IoT для виявлення та відстеження пацієнтів із діабетом 2-го типу. WBAN збирає дані про соціальну взаємодію користувача та про те, як відбуваються емоції та інші фізіологічні зміни. Основними групами даних, які аналізувалися, були діабет типу 2 та неінфіковані особи. У цьому дослідженні було запропоновано гібридну методику, засновану на обох нейроморфних VIKOR тип-2, для поліпшення оцінювання ризику діабету 2-го типу. Отже, можна передбачити основу підтримання прийняття рішень, щоб точно прогнозувати ризики діабету 2-го типу для пацієнтів із результатами дослідження. Якщо користувач вважається «хворим», алгоритм розумно вибере етап, форму та лікування. Такі інтелектуальні алгоритми можуть допомогти мінімізувати час упровадження лікування на 9,8% та покращити показники відновлення пацієнтів у разі серйозних станів здоров'я.

Mavromatis Alex та ін. [9] планують, аналізують та перевіряють нову програмно-визначену систему керування IoT (SDIM) для керування у взаємозв'язаній сенсорній мережі. Систему SDIM оптимізовано для розгортання найсучасніших безпроводових сенсорних мереж (WSN), націлених на щільні розгортання Інтернету речей, де централізоване керування системою не може добре масштабуватися для хмарних WSN. Проте SDIM можна використовувати для хмарного відстеження та контролю всіх доменів IoT, завдяки введеній Агрегації топології програмного забезпечення (SDN) (SDTA). На основі вимірювань ефективності, зокрема часу, необхідного для забезпечення вузлів обчислювального оброблення з кількома доступами (MEC), автори демонструють, що SDIM виконує такі передові схеми керування IoT як у великих емульованих мережах IoT, так і на польових випробуваннях. Відповідна SDIM зменшить середній час забезпечення на 60-80% порівняно з NETCONF Light та на 46-60% порівняно з LWM2M.

Debauche Olivier та ін. [10] визначили нове покоління штучного інтелекту архітектури речі через партнерство, розгорнуте в хмарі з мікросервісами. Окрім використання або розгортання вдосконалених алгоритмів штучного інтелекту (ШІ). Пропоновану архітектуру було проаналізовано з використанням нетрадиційних методів та моделей ШІ, навчених на хмарному сервері, що працює на P100. Потім здійснювався статистичний аналіз вихідних даних вихідної моделі (час висновку) та точності із збіркою тестових даних 443 зображень. Експеримент показав, що Jetson Nano працює повільніше, ніж Tesla P100, а точність зменшується приблизно на 5%.

Результати

Отже, дослідники використовували різні типи методів та інструментів для підвищення точності і продуктивності. Проєкт мав охоплювати порівняння успішності і подібності методології вико-

ристання Інтернету речей із хмарними обчисленнями. Для аналізу результатів науковцями було застосовано інструменти і техніку, а також підхід «важливі досягнуті цілі».

Використання цієї методології і методів дало змогу отримати надійні структури, фрейми і функції, зокрема новий метод міграції віртуальних машин у реальному часі, метод консолідації віртуальних машин з урахуванням робочого навантаження (WAVMCM), стратегію спільного балансування навантаження і розвантаження мобільних граничних обчислень (MEC). Також було запропоновано новий пристрій IoT для ідентифікації та відстеження пацієнтів із діабетом 2-го типу, нову систему Software-Defined IoT Management (SDIM) для керування від взаємозалежної сенсорної мережі. Найкращу точність і ефективність було поліпшено завдяки прогнозованим алгоритмам, зокрема скороченню кількості працюючих серверів на 9%, зниженню енергоспоживання на 15%, прискоренню затримки обслуговування на 59 і 51%, а також загальної відмовостійкості (оцінка 96%). Для порівняння, рівень безпеки залишається вищим за 20%.

ВИСНОВКИ

Останніми роками дедалі зростає інтерес до IoT як з боку наукових кіл, так і бізнес-компаній. Зараз це важлива складова нашого життя. Він може пов'язати майже все у світі людей із навколишнім середовищем. Системи IoT мають складну конструкцію з обмеженими можливостями для зберігання та пошуку. Інтеграція хмарних обчислень мала б багато переваг для значної кількості додатків Інтернету речей.

У статті було досліджено найсучаснішу хмарну інфраструктуру, включно з хмарними функціями, архітектурою та перевагами. Головну увагу було зосереджено на численних технологіях IoT, які розширюватимуться в хмарі. Також було сформульовано проблеми хмарного розгортання IoT та прозорі проблеми.

Загалом, продемонстрований огляд підсумував сучасний внесок у хмарні обчислення та IoT, їх застосування в нашому середовищі, а також проілюстрував потенційні напрямки досліджень і справжні проблеми щодо інтеграції з IoT хмарних обчислень.

Список використаної літератури

*1. **Mohiuddin I., Almogren A.** Workload aware VM consolidation method in edge/cloud computing for IoT applications / IEEE. 2019 [Електронний ресурс]. URL:*

https://www.sciencedirect.com/science/article/abs/pii/S0743731518306762.

*2. **Secure** and Optimized Load Balancing for Multi-Tier IoT and Edge-Cloud Computing Systems / W.-Z. Zhang, I. A. Elgendy, M. Hammad [et al.] // IEEE. 2020 [Електронний ресурс]. URL:*

https://ieeexplore.ieee.org/document/9279239.

*3. **Riad K., Huang T., Ke L.** A dynamic and hierarchical access control for IoT in multi-authority cloud storage. 2020 [Електронний ресурс]. URL:*

https://www.researchgate.net/publication/340372165_A_dynamic_and_hierarchical_access_control_for_IoT_in_multi-authority_cloud_storage.

*4. **IoT enabled** cancer prediction system to enhance the authentication and security using cloud computing / M. Anuradha, T. Jayasankar, N. Prakash [et al.]. 2021 [Електронний ресурс]. URL:*

https://www.researchgate.net/publication/346171393_IoT_enabled_cancer_prediction_system_to_enhance_the_authentication_and_security_using_cloud_computing.

*5. **A volunteer** supported fog computing environment for delaysensitive IoT applications / B. Ali, M. A. Pasha, S. ul Islam [et al.] // IEEE. 2020 [Електронний ресурс]. URL:*

https://ieeexplore.ieee.org/abstract/document/9201470.

*6. **Wang M., Zhang Q.** Optimized data storage algorithm of IoT based on cloud computing in distributed system. 2020 [Електронний ресурс]. URL:*

https://www.researchgate.net/publication/340701668_Optimized_data_storage_algorithm_of_IoT_based_on_cloud_computing_in_distributed_system

*7. **Fuentes H., Mauricio D.** Smart water consumption measurement system for houses using IoT and cloud computing. 2020 [Електронний ресурс]. URL:*

https://www.researchgate.net/publication/343946094_Smart_water_consumption_measurement_system_for_houses_using_IoT_and_cloud_computing.

*8. **A novel** intelligent medical decision support model based on soft computing and IoT / M. Abdel-Basset, G. Manogaran, A. Gamal, V. Chang // IEEE. 2019 [Електронний ресурс]. URL:*

https://ieeexplore.ieee.org/document/8787865.

*9. **A softwaredefined** IoT device management framework for edge and cloud computing / A. Mavromatis, C. Colman-Meixner, A. P. Silva [et al.] // IEEE. 2019 [Електронний ресурс]. URL:*

https://ieeexplore.ieee.org/document/8883180.

*10. **A new** edge architecture for ai-iot services deployment / O. Debauche, S. Mahmoudi, P. Manneback [et al.]. 2020 [Електронний ресурс]. URL:*

https://www.researchgate.net/publication/340256484_A_new_Edge_Architecture_for_AI-IoT_services_deployment.

М. А. Макарцев, А. Н. Тушич, И. В. Замрий, Л. Т. Алексина

ПРОБЛЕМЫ, ТРУДНОСТИ И ВОЗМОЖНОСТИ IoT И ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

С развитием Индустриального Интернета вещей (IIoT) наблюдается постоянный рост объема информации. Однако нецелесообразно хранить все необработанные данные в устройствах IIoT, поскольку энергия конечных устройств не исчерпывающая, а дополнительные помещения жестко ограничены. Сети IoT расширяют возможности присвоенного ассортимента информации и распределенного хранилища независимо от искусственной природы IoT. Существует ряд неопределенных гарантий проблем IoT и интеграции в облако. Облачные вычисления высокоэффективны, хранение становится все более актуальным, и некоторые группы сейчас передают свои данные из собственных записей в центры поставщиков облачных вычислений. Интенсивные программы IoT для рабочих нагрузок и данных могут привести к трудностям при использовании распределенных вычислительных аппаратов. В статье исследованы IoT и облачные вычисления, а также рассмотрены совместимые с облаком проблемы и вычислительные техники для содействия стабильному переходу программ IoT к облаку.

Ключевые слова: Интернет вещей; IoT; облачные вычисления; безопасность; IoT-облако.

M. O. Makartsev, A. M. Tushych, I. V. Zamryi, L. T. Alexina

IoT AND CLOUD COMPUTING ISSUES, DIFFICULTIES AND OPPORTUNITIES

The Cloud is a centralised system that helps to deliver and transport data and various files across the Internet to data centres. The different data and programmes can be accessed easily from the centralised Cloud system. Cloud Computing is an economic solution, as it does not require on-site infrastructure for storage, processing and analytics. The scalability of Cloud Computing means that as your business grows, your technological and analytical capabilities can too.

The relationship between IoT, Big Data and Cloud Computing creates ample opportunity for business to harness exponential growth. Put simply, IoT is the source of data, Big Data is an analytic platform of data, and Cloud Computing is the location for storage, scale and speed of access.

The Internet of Things refers to the world's collection of devices that gather and share information across various industries and sectors. In comparison, Big Data offers management and analytical capabilities for huge amounts of data across multiple platforms and systems. However, the interconnectivity between Big Data and Internet of Things means the two technologies share common goals and are predicted to follow a similar trajectory in the future.

With the outstanding development of the Industrial Internet of Things (IIoT), various outlets continually produce a tremendous volume of information. It is unwise to locally store all the raw data in the IIoT devices since the end devices energy, and extra rooms are rigorously constrained. IoT networks empower re-appropriated information assortment and distributed storage regardless of the asset compelled nature of the IoT. For the following section of observation, there is a succession of unfamiliar safeguards for IoT and cloud integration problems. Cloud computing delivery is highly efficient, storage is becoming more and more current, and some groups are now transfering their data from in-house records to Cloud Computing Vendors hubs. Intensive IoT applications for workloads and data are liable to challenges while using distributed computing apparatuses. In this paper, we research IoT and cloud computing and address cloud-compatible problems and computing techniques to promote IoT programs stable transition to the Cloud.

Keywords: Internet of Things; IoT; Cloud Computing; Security; IoT-cloud.