Облікова картка НДДКР

Державний обліковий номер: 0223U004785

Державний реєстраційний номер: 0123U103640

Відкрита

Дата реєстрації: 04-12-2023

1. Етапи виконання

Номер етапу: 1

Назва етапу: Теоретичний аналіз і формулювання гіпотез (3 місяці)

Початок етапу: 09-2023

Закінчення етапу: 01-2024

Вид звітного документа: Проміжний звіт

2. Виконавець

Назва організації: Київський національний університет будівництва і архітектури

Код ЄДРПОУ/ІПН: 02070909

Підпорядкованість: Міністерство освіти і науки України

Адреса: проспект Повітрофлотський, буд. 31, м. Київ, 03037, Україна

Телефон: 380442415580

E-mail: knuba@knuba.edu.ua

WWW: http://www.knuba.edu.ua/

3. Власник результатів НДДКР (продукції)

Назва організації: Київський національний університет будівництва і архітектури

Код ЄДРПОУ/ІПН: 02070909

Адреса: проспект Повітрофлотський, буд. 31, м. Київ, 03037, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380442415580

E-mail: knuba@knuba.edu.ua

WWW: http://www.knuba.edu.ua/

4. Джерела та напрями фінансування

Підстава для проведення робіт: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

КПКВК:

Напрям фінансування: 2.1 - фундаментальні дослідження

Джерела фінансування

Джерело фінансування: 7704 - власні кошти, кошти підприємств, установ, організацій, фізичної особи на виконання ініціативних робіт

Фактичний обсяг фінансування за звітний етап: 3.000 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Методи і моделі забезпечення безпеки та діагностики критичних параметрів у складних системах з використанням IoT

Назва роботи (англ)

Methods and models for ensuring safety and diagnosing critical parameters in complex systems using IoT

Реферат (укр)

Забезпечення безпеки систем діагностики критичних режимів у складних системах, використовуючи Інтернет речей (IoT), є важливою проблемою в сучасному світі, оскільки складні системи стають все більш залежними від цифрових технологій. У цьому контексті важливо проаналізувати різні методи та моделі для забезпечення надійної та безпечної роботи таких систем. Системи IoT включають в себе велику кількість різноманітних пристроїв, які взаємодіють між собою через мережу Інтернет. Ці системи можуть бути застосовані в багатьох галузях, таких як медицина, автопромисловість, енергетика та багато інших. Однак разом з їхніми перевагами приходять і загрози для безпеки. Діагностика критичних режимів систем є критично важливою для попередження можливих аварій та збоїв. Методи та моделі для забезпечення безпечної діагностики включають в себе використання алгоритмів машинного навчання, аналізу даних, інтернет-аналізу вещей та багато інших підходів. Однак, важливо враховувати потенційні загрози та вразливості цих систем, які можуть бути використані зловмисниками для введення в оману, атаки на конфіденційні дані або завдання збитків. Однією з основних задач у забезпеченні безпеки систем IoT є розробка механізмів виявлення та відповіді на потенційні загрози. Це може включати в себе створення систем моніторингу та аналізу, які можуть вчасно виявляти аномалії та потенційні атаки. Крім того, важливо розробити стратегії забезпечення конфіденційності, цілісності та доступності даних у системах IoT. У висновку, забезпечення безпеки систем діагностики критичних режимів у складних системах з використанням IoT є важливою задачею в сучасному світі. Для досягнення цієї мети необхідно використовувати різні методи та моделі, розробляти механізми виявлення та відповіді на загрози, а також забезпечувати конфіденційність, цілісність та доступність даних. Це важливо для забезпечення безпеки та надійності сучасних IoT-систем.

Реферат (англ)

Ensuring the security of critical mode diagnosis systems in complex systems using IoT is an important issue in the modern world, as complex systems are becoming increasingly reliant on digital technologies. In this context, it is important to analyze various methods and models to ensure the reliable and safe operation of such systems. IoT systems encompass a wide range of diverse devices that interact with each other through the Internet network. These systems can be applied in various fields such as medicine, automotive industry, energy, and many others. However, along with their advantages, come threats to security. The diagnosis of critical modes in systems is crucial for preventing potential accidents and failures. Methods and models for ensuring secure diagnostics include the use of machine learning algorithms, data analysis, Internet of Things analysis, and many other approaches. However, it is important to consider potential threats and vulnerabilities of these systems that can be exploited by malicious actors for deception, data breaches, or causing damage. One of the primary tasks in IoT system security is the development of mechanisms for detecting and responding to potential threats. This may involve creating monitoring and analysis systems capable of timely identifying anomalies and potential attacks. Additionally, it is crucial to develop strategies to ensure data confidentiality, integrity, and availability in IoT systems. In conclusion, ensuring the security of critical mode diagnosis systems in complex systems using IoT is an important task in the modern world. To achieve this goal, various methods and models must be employed, mechanisms for threat detection and response must be developed, and data confidentiality, integrity, and availability must be ensured. This is essential for the safety and reliability of modern IoT systems.

Індекс УДК: 654.1; 654.14; 654.15; 654.16; 654.17; 654.19; 656.8, 621.865.8, , 550.34.033 , 004.8'2:621.395

Коди тематичних рубрик НТІ: 49.33.35, 55.30, 20.56, 37.01.51

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Методи класифікації режимів та статусів технічної системи за категоріями: некритичний, критичний та суперкритичний

Назва продукції (англ): Methods of classifying modes and statuses of a technical system into categories: non-critical, critical, and supercritical

Очікувані результати: Методи, теорії

Галузь застосування: комп'ютерні науки

Опис продукції (укр): Методи класифікації режимів і статусів технічної системи за категоріями "не критичний", "критичний" і "суперкритичний" є важливими для ефективного управління та підтримки таких систем. Ці методи допомагають визначити, наскільки серйозні або критичні проблеми або події можуть вплинути на нормальну роботу технічної системи. Нижче наведено огляд можливих методів класифікації: Оцінка ризику: Один з найпоширеніших методів полягає в оцінці ризику для конкретного статусу системи. Ризик визначається на основі ймовірності виникнення події та її потенційних наслідків. Зазвичай системи розділяють на кілька рівнів ризику, таких як "низький", "середній" і "високий", щоб визначити ступінь критичності. Аналіз вразливостей: Цей метод передбачає визначення вразливостей системи і їх впливу на функціонування. Вразливості, які можуть призвести до некритичних проблем, розглядаються в інший спосіб, ніж ті, які можуть створити критичні або суперкритичні ситуації. Оцінка відновлюваності: Цей метод включає в себе оцінку того, наскільки швидко і легко можна відновити систему після виникнення проблеми. Чим швидше можна відновити систему, тим менше вона схильна до суперкритичних статусів. Моніторинг і виявлення подій: Використання систем моніторингу і виявлення подій допомагає вчасно виявляти аномалії або потенційні загрози. Це дозволяє класифікувати статус системи на ранніх етапах і запобігати погіршенню ситуації. Стандарти та регулювання: У деяких випадках стандарти та регулювання визначають, які критерії повинні бути використані для класифікації систем за ступенем критичності. Наприклад, в галузі безпеки інформації існують стандарти, які визначають рівень важливості для інформації. Методика аналізу впливу і можливості (Impact and Probability Analysis): Цей метод включає в себе оцінку впливу можливих подій на систему і вірогідності їхнього виникнення. Це дозволяє визначити ризик і класифікувати статус системи.

Соціально-економічна спрямованість НТП: Економія матеріалів, Зменшення зносу обладнання, Підвищення автоматизації виробничих процесів

Стадія завершеності НТП: Ідея, концепція

Впровадження НТП: Не впроваджено

Строки впровадження: 09.202311.2023

Виробник продукції: Київський національний університет будівництва і архітектури

Споживачі продукції:

Перспективні ринки:

Права інтелектуальної власності: За договорами, В Україні

Форми та умови передачі продукції: Навчання персоналу

7. Бібліографічний опис

1. Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. IEEE Wireless Communications, 23(5):10–16, 2016. 2. Jennifer B´elissent et al. Getting clever about smart cities: New opportunities require new business models. Cambridge, Massachusetts, USA, 193:244–77, 2010. 3. Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos. Machine learning based solutions for securit

2. Jennifer B´elissent et al. Getting clever about smart cities: New opportunities require new business models. Cambridge, Massachusetts, USA, 193:244–77, 2010.

3. Syeda Manjia Tahsien, Hadis Karimipour, and Petros Spachos. Machine learning based solutions for security of internet of things (IoT): A survey. Journal of Network and Computer Applications, 161:102630, 2020.

4. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4):2347–2376, 2015.

5. Sarker, Iqbal H., Asif Irshad Khan, Yoosef B. Abushark, and Fawaz Alsolami. "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions." Mobile Networks and Applications, March 14, 2022.

6. H. Zhang and L. Zhu, “Internet of things: Key technology, architecture and challenging problems,” in 2011 IEEE International Conference on Computer Science and Automation Engineering, vol. 4. IEEE, 2011, pp. 507–512.

7. L. Li, “Study on security architecture in the internet of things,” in Proceedings of 2012 International Conference on Measurement, Information and Control, vol. 1. IEEE, 2012, pp. 374–377.

8. J.-H. Han, Y. Jeon, and J. Kim, “Security considerations for secure and trustworthy smart home system in the iot environment,” in 2015 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, 2015, pp. 1116–1118.

9. M. Schiefer, “Smart home definition and security threats,” in 2015 ninth international conference on IT security incident management & IT forensics. IEEE, 2015, pp. 114–118.

10. C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, and H. D. Hai, “Recent challenges, trends, and concerns related to iot security: An evolutionary study,” in 2018 20th International Conference on Advanced Communication Technology (ICACT). IEEE, 2018, pp. 405–410.

11. M. Alrowaily and Z. Lu, “Secure edge computing in iot systems: Review and case studies,” in 2018 IEEE/ACM Symposium on Edge Computing (SEC). IEEE, 2018, pp. 440–444.

12. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for iot security based on learning techniques,” IEEE Communications Surveys & Tutorials, 2019.

13. J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

14. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

15. J. Kim and H. Kim, “Security vulnerability and considerations in mobile rfid environment,” in 2006 8th International Conference Advanced Communication Technology, vol. 1. IEEE, 2006, pp. 801–804.

16. I. Bedhief, M. Kassar, and T. Aguili, “Sdn-based architecture challenging the iot heterogeneity,” in 2016 3rd Smart Cloud Networks & Systems (SCNS). IEEE, 2016, pp. 1–3.

17. K. Kalkan and S. Zeadally, “Securing internet of things (iot) with software defined networking (sdn),” IEEE Communications Magazine, no. 99, pp. 1–7, 2017.

18. L. Sidki, Y. Ben-Shimol, and A. Sadovski, “Fault tolerant mechanisms for sdn controllers,” in 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). IEEE, 2016, pp. 173–178.

19. Z. Shi, K. Liao, S. Yin, and Q. Ou, “Design and implementation of the mobile internet of things based on td-scdma network,” in 2010 IEEE International Conference on Information Theory and Information Security. IEEE, 2010, pp. 954–957.

20. A. W. Atamli and A. Martin, “Threat-based security analysis for the internet of things,” in 2014 International Workshop on Secure Internet of Things. IEEE, 2014, pp. 35–43.

21. M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016.

22. C. Tumrongwittayapak and R. Varakulsiripunth, “Detecting sinkhole attack and selective forwarding attack in wireless sensor networks,” in 2009 7th International Conference on Information, Communications and Signal Processing (ICICS). IEEE, 2009, pp.

1–5.

23. E. Bou-Harb, M. Debbabi, and C. Assi, “Cyber scanning: a comprehensive survey,” IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1496–1519, 2014.

24. Zhang, Jian, Huaijian Chen, Liangyi Gong, Jing Cao, and Zhaojun Gu. "The Current Research of IoT Security." In 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC). IEEE, 2019.

25. Opirskyy, Ivan, Roman Holovchak, Iryna Moisiichuk, Tetyana Balianda, and Sofiia Haraniuk. 2021. “PROBLEMS AND SECURITY THREATS TO IOT DEVICES”. Electronic Professional Scientific Edition «Cybersecurity: Education, Science, Technique» 3 (11):31-42.

8. Звітна документація

Кількість сторінок в звіті: 67

Мова звіту: Українська

Умови поширення в Україні: Не заборонено

Умови передачі іншим країнам: Не заборонено

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Власенко Мирослава Юріївна

Делембовський Максим Михайлович (к. т. н.)

Касім Намір Намір (к. т. н.)

Кондакова Анастасія Юріївна

Хлапонін Юрій Іванович (д. т. н.)

Шабала Євгенія Євгеніївна (к. т. н.)

Керівник організації:

Хлапонін Юрій Іванович (д. т. н., професор)

Керівники роботи:

Гуменний Дмитро Олександрович (к.т.н., доц.)

Делембовський Максим Михайлович (к. т. н., доцент)

Хлапонін Юрій Іванович (д. т. н., професор)

Шабала Євгенія Євгенівна (к. т. н., доцент)

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.