AXBOROT TIZIMLARIDA KIRISHNI ANIQLASH MODELLARINI ISHLAB CHIQISHNING AQLLI USULLARI

Begimov O‘ktam Ibragimovich
Alfraganus university “Raqamli texnologiyalari” kafedra mudiri
uktambegimov24@gmail.com
Jovliyev Ulug‘bek Davronovich
Alfraganus university “Raqamli texnologiyalari” fakulteti magistri

Annotatsiya: Ushbu maqola axborot tizimlarida kirishni aniqlash modellarini avtomatik ravishda qurishning aqlli usullarini tahlil qiladi. Kirishni aniqlash modellarining ikki asosiy turi-imzolash asosida va anomaliyalarga asoslangan-keltirilgan. Maqolada avtomatik model qurish jarayonining to‘rt asosiy bosqichi: ma’lumot to‘plash, ma’lumotlarni oldindan qayta ishlash, model qurish va uning baholanishi va optimallashtirilishi ko‘rib chiqiladi. Mashinani o‘rganish va chuqur o‘rganish kabi zamonaviy texnologiyalar, shuningdek, natijalarga asoslangan o‘rganish usullari yordamida kirishni aniqlash samaradorligini oshirish mumkinligi ta'kidlangan. Ushbu tadqiqot, axborot tizimlarining xavfsizligini kuchaytirish va ruxsatsiz kirishlarni oldini olishda zamonaviy yechimlarni taklif etadi.

Kalit so‘zlar: Axborot tizimlari, kirishni aniqlash modellar, avtomatik qurish, aqlli usullar, mashinani o‘rganish, chuqur o‘rganish, anomaliyalarga asoslangan model, imzolash asosidagi model, ma’lumot to‘plash, ma’lumotlarni qayta ishlash, modelni baholash va optimallashtirish, xavfsizlik, ruxsatsiz kirish, hujumlardan himoya.

Annotation: This article analyzes intelligent methods for automatically building intrusion detection models in information systems. Two main types of intrusion detection models-signature based and anomaly-based are presented. The article examines the four main steps of the automatic model building process: data collection, data preprocessing, model building, and its evaluation and optimization. It is noted that the effectiveness of intrusion detection can be improved with the help of modern technologies such as machine learning and deep learning, as well as results-based learning methods. This study offers modern solutions to strengthen the security of information systems and prevent unauthorized access.

Keywords: Information systems, intrusion detection models, automatic construction, intelligent methods, machine learning, deep learning, anomaly-based model, signature-based model, data mining, data processing, model evaluation and optimization, security, protection against unauthorized access, attacks.

Аннотация: В данной статье анализируются интеллектуальные методы автоматического построения моделей обнаружения вторжений в

информационных системах. Приводятся два основных типа моделей обнаружения вторжений - на основе сигнатур и на основе аномалий. В статье рассматриваются четыре основных этапа процесса автоматического построения модели: сбор данных, предварительная обработка данных, построение модели, ее оценка и оптимизация. Отмечается, что эффективность обнаружения вторжений можно повысить с помощью современных технологий, таких как машинное обучение и глубокое обучение, а также методов обучения, основанного на результатах. В данном исследовании предлагаются современные решения для усиления безопасности информационных систем и предотвращения несанкционированного доступа.

Ключевые слова: Информационные системы, модели обнаружения вторжений, автоматическое построение, интеллектуальные методы, машинное обучение, глубокое обучение, модель на основе аномалий, модель на основе сигнатур, интеллектуальный анализ данных, обработка данных, оценка и оптимизация модели, безопасность, защита от несанкционированного доступа, атаки.

Axborot tizimlari har doim muhim axborotlarni saqlash va ularga kirishni boshqarish bilan bog‘liq. Kirishni aniqlash modellari (KAM) bu tizimlarga hujumlardan himoya qilish va ruxsatsiz kirishlarni oldini olishda muhim rol o‘ynaydi. Ushbu maqolada, axborot tizimlarida kirishni aniqlash modellarini avtomatik ravishda qurish uchun zamonaviy aqlli usullar tahlil qilinadi.

Kirishni aniqlash modellari ikki asosiy turga bo‘linadi: imzolash asosida va anomaliyalarga asoslangan. Imzolash asosida ishlovchi modellarda, oldindan belgilangan qoidalar va imzolar yordamida kirish faoliyatlari tahlil qilinadi. Aksincha, anomaliyalarga asoslangan modellarda, normal faoliyatdan chetga chiqqan xatti-harakatlar aniqlanadi.

Avtomatik qurish jarayoni

Ma’lumot to‘plash. Kirishni aniqlash modellari uchun ma’lumot to‘plash jarayoni birinchi bosqichdir. Bu jarayon avtomatik ravishda turli manbalardan (tarmoq trafigi, log fayllar va boshqalar) ma’lumotlarni yig‘ishni o‘z ichiga oladi. Ma’lumotlar to‘plami sifatida tahlil qilish uchun etarlicha katta va xilma-xil bo‘lishi zarur.

Ma’lumotlarni oldindan qayta ishlash. Yig‘ilgan ma’lumotlar oldindan qayta ishlanishi kerak. Bu jarayonda shovqinlarni olib tashlash, normalizatsiya va xususiyatlarni ajratish kabi amallar amalga oshiriladi. Ma’lumotlar to‘g‘riligini ta’minlash kirishni aniqlash samaradorligini oshiradi.

Model qurish. Avtomatik model qurish jarayoni mashinani o‘rganish (MO) va chuqur o‘rganish (CO) algoritmlaridan foydalanadi. Masalan, qaror daraxtlari, neyron tarmoqlar va boshqa algoritmlar yordamida kirishni aniqlash modellarini yaratish

mumkin. Ushbu algoritmlar ma’lumotlar to‘plamidan o‘rganib, kelajakdagi xatti-harakatlarni oldindan bashorat qilish imkonini beradi.

Modelni baholash va optimallashtirish. Qurilgan modelning samaradorligini baholash uchun uni test ma’lumotlari bilan sinovdan o‘tkazish zarur. Baholash natijalari asosida modelni optimallashtirish, ya’ni parametrlarni o‘zgartirish va algoritmni yaxshilash amalga oshiriladi. Bu jarayon avtomatik ravishda o‘zgarishi mumkin.

Aqlli usullar

1. Mashinani o‘rganish. Mashina o‘rganish algoritmlari yordamida kirishni aniqlash modellari yaratish jarayoni avtomatlashtiriladi. Bu algoritmlar avvalgi ma'lumotlarga asoslanib, yangi kiritishlarga javob berishni o‘rganadi.

2. Chuqur o‘rganish. Chuqur o‘rganish texnologiyalari murakkab xatti-harakatlarni aniqlashda samarali. Neyron tarmoqlari yordamida anomaliyalarni aniqlash va ularga mos ravishda model qurish mumkin.

3. Natijalarga asoslangan o‘rganish. Bu usul, modelning natijalaridan o‘rganib, yangi strategiyalar ishlab chiqishga imkon beradi. Natijalarga asoslangan o‘rganish jarayonida model doimiy ravishda o‘zini yangilab boradi.

Xulosa

Axborot tizimlarida kirishni aniqlash modellarini avtomatik ravishda qurish aqlli usullar yordamida samaradorligini oshiradi. Ushbu jarayon, ma’lumotlarni to‘plashdan tortib, modelni baholash va optimallashtirishgacha bo‘lgan bosqichlarni o‘z ichiga oladi. Kelajakda bu usullar yanada rivojlanib, axborot tizimlarining xavfsizligini yanada kuchaytirishga yordam beradi.

Avtomatik qurish jarayonidagi aqlli usullar nafaqat samaradorlikni oshiradi, balki tizimlar xavfsizligini ham kuchaytiradi. Kelajakda bu usullarni yanada rivojlantirish, shuningdek, ularni real vaqt rejimida qo‘llash, axborot tizimlarining xavfsizlik darajasini yanada oshirishga yordam beradi. Shunday qilib, kirishni aniqlash modellarini ishlab chiqish va ularni yangilash jarayonlari axborot tizimlarining mudofaasini mustahkamlashda muhim ahamiyatga ega bo‘ladi.

Axborot tizimlarida kirishni aniqlash modellarini avtomatik ravishda qurish zamonaviy xavfsizlik strategiyalarining ajralmas qismidir. Ushbu maqolada tahlil qilingan usullar, masalan, mashinani o‘rganish va chuqur o‘rganish, kirish faoliyatlarini samarali aniqlash va ruxsatsiz kirishlarni oldini olishda katta imkoniyatlar taqdim etadi. Model qurish jarayoni ma’lumotlarni to‘plashdan boshlab, ularni qayta ishlash, modellash va baholashgacha bo‘lgan bir qator bosqichlarni o‘z ichiga oladi.

Foydalanilgan adabiyotlar.

1. Bishop, C. M., Pattern Recognition and Machine Learning. Springer, 2006.
2. Goodfellow, I., Bengio, Y., & Courville, A., Deep Learning. MIT Press, 2016.

3. Hodge, V. J., & Austin, J., “A survey of outlier detection methodologies” Artificial Intelligence Review, 22(2), 2004, 85-126.
4. Tan, P. N., Steinbach, M., & Kumar, V. (2019). Introduction to Data Mining. Pearson.
5. Zhou, Z.-H., Ensemble Methods: Foundations and Algorithms. CRC Press, 2012.
6. Sommer, P., & Paxson, V., “Outside the closed world: On using machine learning for network intrusion detection”, IEEE European Symposium on Security and Privacy, 2010, 305-320.
7. Li, W., & Li, Q., “Anomaly detection based on deep learning: A survey”, International Journal of Information Security, 17(6), (2018), 599-619.
8. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). “A survey of network anomaly detection techniques”, Journal of Network and Computer Applications, 60, 201-217.
9. Zhang, Y., & Zheng, Y.,“A deep learning approach for intrusion detection”, Journal of Information Security and Applications, 42, (2018) 150-157.
10. Kull, M., & Flach, P., “Beyond accuracy: F-measure, the lack of consistency and the importance of being precise”, Machine Learning, 95(2), (2014), 203-234.