iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

THE ROLE OF DEVSECOPS IN FINANCIAL AI MODELS: INTEGRATING SECURITY AT EVERY STAGE OF AI/ML MODEL DEVELOPMENT IN BANKING AND INSURANCE

Nihar Malali
Senior Solutions Architect, UT Dallas

ABSRACT
Artificial intelligence (AI) and machine learning (ML) technologies have brought revolutionary changes to financial institutions such as banks and insurers during their operations. The financial industry relies heavily on AI models for both automated underwriting policies and personalized recommendation services and fraudulent activity discovery along with credit scoring assessments. The deeper financial institutions incorporate these models into their systems them more vulnerability to cyberattacks. DevSecOps represents a revolutionary method which includes security measures during every stage of development from the initial phase through the final phase of AI/ML model lifecycle. This paper investigates how DevSecOps secures financial AI models while discussing the special digital threats faced by banking and insurance institutions. Security considerations need to be embedded throughout the entire data preprocessing to deployment cycle due to their roles in ensuring regulatory adherence, safeguarding sensitive information and preserving dependability.
The document utilizes five sections to present information about DevSecOps events in financial AI systems and development pipeline security approaches as well as deployment risk reduction techniques and compliance requirements together with successful implementation examples. This work provides organizations with a real-world approach for developing resilient and compliant AI systems which benefits data specialists along with practitioners from financial IT teams. Minimizing risk takes precedence over convenience because modern financial institutions operate with extensive data sets and serious consequences making DevSecOps implementation mandatory. Security as a baseline framework before consideration of anything else allows institutions to protect both customer trust along with institutional integrity while ensuring their AI initiatives have enduring value.

Keywords:
DevSecOps, Financial AI Models, AI/ML Security, Data Privacy, Model Risk Management

1. INTRODUCTION TO DEVSECOPS IN FINANCIAL AI

Artificial Intelligence (AI) and Machine Learning (ML) fundamentally change financial operations especially in banking combined with insurance services. AI/ML models transform banking institutions because they enable improved assessments of risks and service optimization together with enhanced decision-making capabilities (Kumar, Taylor & Wong, 2017; Jain, 2017). These complex models provide growing security risks and explainability limitations for bias and compliance which exceed the capabilities of traditional software development models (Holzinger et al., 2018).
The surge of software delivery requirements directed developers to establish DevOps as a culture-based cooperation model between software developers and IT operators. The growing number of sophisticated security incidents drove DevOps development toward the creation of DevSecOps which established security responsibility throughout the entire development life cycle (Crespo, Kumar & Noteboom, 2017; Kazi & Saniora, 2019). Financial AI models require this switch beyond being merely a best practice because it constitutes a necessary operational requirement. DevSecOps creates a development pathway which inserts security practices together with compliance and governance requirements throughout the complete modeling life cycle starting from data collection until deployment monitoring.
Financial institutions experience high risk from model exploitation together with adversarial attacks leading to data breaches and credit errors plus market prediction manipulation and discriminatory outcomes (Bennett, 2017; Díaz et al., 2019). The resulting failures endanger customer confidence while creating major financial losses and damaging organizational reputation. Regulatory authorities closely watch financial decisions made by AI systems

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

due to their central role and they expect more excellent standards in explainability development and robustness and fairness delivery. Financial services are adopting responsible AI practices by following the guidelines from the EU AI Act together with the FSB's framework on AI in financial institutions (Financial Stability Board, 2017). DevSecOps is a vital method for generating protected resilient and standard-compliant AI systems in this environment. Such a security culture allows vulnerabilities to be spotted early through continuous monitoring during the entire model lifecycle. Financial institutions implement risk management goals through security controls and governance frameworks when they incorporate these elements during all stages of the AI/ML pipeline development through a DevSecOps approach. This paper reveals that financial organizations should implement DevSecOps methods for AI model development because the approach defends trustworthiness alongside regulatory obedience and algorithmic decision integrity within data-driven economic frameworks.

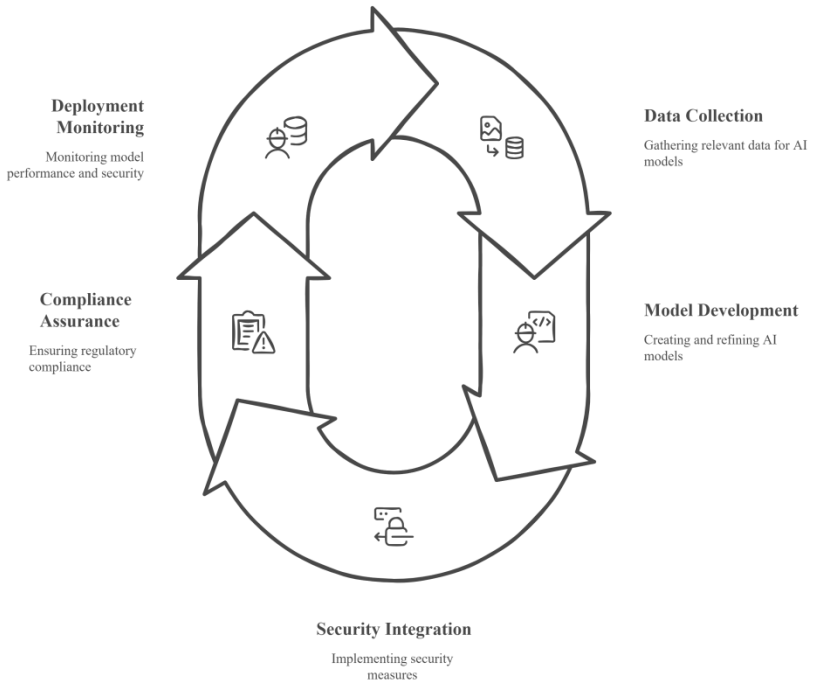

Figure 1: DevSecOps Cycle for Financial AI

2. BUILDING A SECURE AI/ML PIPELINE: DEVSECOPS PRINCIPLES APPLIED

Financial sector AI/ML models must achieve accuracy and compliance standards as well as maintenance security protocols along with mechanisms for explainable system practices. Applying DevSecOps allows security to be embedded in the complete model life cycle from data ingestion through deployment while reducing the risks that occur in crucial banking and insurance operations.

- **Shift-left security in data collection and preprocessing**

Data security emerges from the first step of implementing secure pipelines during the data privacy and integrity processes. Financial organizations treat PII data within their databases as high-value targets because those records present direct opportunities for cybercriminals to gain unauthorized access. Security measures at the early phase of data processing involve validating sources and using cryptographic hashing along with methods like differential privacy or data masking for privacy protection (Cobb, 2016; Mehmood et al., 2016). These security practices when included in the pipeline will protect the model from using corrupted data during downstream operations.

- **Automated security testing in model development**

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

The implementation of automated tools operates during development to scan for secret credentials while analyzing code static elements and evaluating container vulnerabilities. Prior to model training models these tools detect insecure configurations and hardcoded credentials together with third-party dependency flaws (Kazi & Saniora, 2019; Díaz et al., 2019). Security gates remain valid due to integrating these tools with version control hooks.

- **Integrity and audibility of model training**

The regulatory standards force organizations to maintain complete visibility in the history of their financial model. Research experiments need to produce identical results and maintain a comprehensive documentation record. Software frameworks MLflow together with DVC allow the tracking of code versions alongside dataset snapshots along with hyperparameters and evaluation metrics within a single system. The implementation of these tools enhances the transparency level together with external audit response capabilities (Bennett, 2017; De Almeida et al., 2017).

- **Secure coding practices for model pipelines**

All authorized agents should receive only the necessary privileges to access data and code through the principle of least privilege. Financial institutions can minimize data security threats through secure API gateways that supplement encryption at rest and in transit and automated code scanning detection systems (Díaz et al., 2019). Seditious operations that include model retraining and data merging need to be stored inside hardened containers which maintain their unmodified state.

- **CI/CD with embedded security protocols**

Financial institutions which use CI/CD for AI deployments need to integrate compliance scanning alongside adversarial robustness evaluation and explanation validation operations into their automated release systems. DevSecOps enables the deployment of tested and compliant, and robust models into production environments according to Prates et al. (2019) and Rahul (2019). Model governance receives additional protection through deployment logs accompanied by canary releases and rollback mechanisms.

DevSecOps implements security protection across all development stages thus both predicting security risks and uniting AI creation with regulatory rules tailored to individual industries (Dagoumas et al., 2017; Holzinger et al., 2018).

3. ADDRESSING RISKS DURING MODEL DEPLOYMENT AND OPERATIONS

Once financial AI models go live they need to resist security threats that change along with system use and data updates. Security functions are built directly within model operations through DevSecOps methods that maintain defence at all times instead of allowing security checks only after issues arise.

Threat Modeling in Financial AI Systems:

- Threat modeling finds specific weaknesses that AI banking and insurance systems have such as unauthorized model hacking or malicious data manipulation.
- The risk of model automation is greatest during credit scoring fraud and claims handling activities.

Preventing Data Leakage and Adversarial Attacks:

- AI systems have the unintended side effect of showing private training data by revealing their predictions and gradient-based information. To protect against model compromise firms use various security procedures such as limiting access permissions and encrypting data plus making output values difficult to understand.
- When attackers manipulate inputs into models they make the system create false reports or let items bypass safety controls. To defend against threats you need to test your systems regularly plus train them to resist attacks and validate incoming data as stated by Holzinger et al. in 2018.

Real-Time Model Monitoring and Threat Detection:

- With DevSecOps methods engineers bring monitoring instruments into every update to keep an eye on system behavior after deployment by detecting performance jumps or unauthorized actions.
- Anomaly detection systems find security problems and model performance issues immediately so security and ML teams can respond fast (Díaz et al., 2019).

Continuous Model Monitoring System

- When financial settings transform due to official rules, market behavior, and market swings the predictions need to be adjusted to match these changes effectively.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

- Company teams can detect financial environment changes faster by using automated system checks and bias testing during the DevSecOps cycle. This helps banks apply for loans or underwrite accounts fairly (De Almeida et al., 2017).

Incident Response and Rollback Mechanisms:

- If a security issue affects the model a fast automatic system needs to undo recent model updates. Teams can easily return to a safe version that keeps the business operations running smoothly.
- DevSecOps pipelines maintain trackable updates plus test results and monitoring tools to conduct safe and trackable system backtracking.
- To meet regulations insurers and bankers should have an established incident response plan with rules to identify causes of failure plus steps for legal communication (Bennett, 2017).

When you apply these methods they change model operations from simple work transfer to an active process through continuous checking of financial AI.

4. REGULATORY COMPLIANCE, GOVERNANCE, AND ETHICS

Financial institutions using AI for decision-making must follow legal rules because this functional element has become essential for allowing AI investments. DevSecOps offers businesses a clear path to make AI/ML systems meet hard regulations about ethics and governance.

Key Regulatory Frameworks:

- AI systems in financial services must fulfil the data protection terms set by GDPR while handling payment security under PCIDs and SOC 2 standards and banking risk oversight as per Basel III.
- The required frameworks expect the AI models to protect personal data while safely processing it and to track all changes that follow industry best practices throughout their lifecycle.

Model Explainability and Auditability:

- Government authorities require models to show how they work especially for uses in loan processing and insurance policy determination. It is impossible to audit black-box artificial intelligence systems because their internal reasoning cannot be understood.
- CLEAR-Trade as described in Kumar et al. (2017) demonstrates how explainable AI provides decision transparency and helps authorities conduct audits. DevSecOps pipelines utilize automation to record and establish versions which enable users to track system activity.

Ensuring Fairness, Transparency, and Accountability:

- Special audits for fairness must operate continuously across product development to find and solve unfair results in lending processes and predictive systems.
- Having clear system operations represents both technical requirements and moral expectations. Research shows that AI systems need to follow responsible decision-making processes and must adhere to rules in controlled industry sectors (Mai, 2016).
- DevSecOps helps organizations add built-in ethical and compliance tests that examine models before they reach production.

Automating Compliance through DevSecOps:

- Using DevSecOps helps incorporate access control measures along with encryption rules and conducts secure code checks during the CI/CD process to produce appropriate documentation.
- DevSecOps includes automated tools to help organizations meet GDPR requirements of “right to explanation” through model output analysis and easy-to-understand information that goes directly into production workflows (Soria-Comas & Domingo-Ferrer, 2016).

Governance Frameworks for Secure AI:

- Governance frameworks succeed when they put together company procedures with system restrictions to regularly check that people manage and monitor risk plus quality outcomes.
- De Almeida et al. (2017) suggest using multiple criteria to make decisions that reduce risk while staying affordable and complying with standards per company strategies.

Through DevSecOps compliance transitions from a one-time task to permanent measured operations which enable banks to expand their AI use safely despite official rules.

5. CASE STUDIES AND BEST PRACTICES IN BANKING & INSURANCE

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Institutions that want to use AI in finance without security risks must adopt DevSecOps as an essential practice. This prominent retail bank created a fraud fighting system based on AI by processing transaction information from millions of accounts at high speed. Through worldwide security implementation of DevSecOps tools the bank decreased false alarms and strengthened its prompt response process. The deployment expanded operational precision and protected the institution from financial regulatory violations according to Dagoumas et al. (2017). One international insurance company redesigned its underwriting service through ML models trained on applicants' information alongside specifics of previous claims and risk types, by adopting DevSecOps procedures and tools like fairness validation tools the company guaranteed output compliance with regulations focused on non-discriminatory standards even after updating its models through safe pipelines. Our system detected changes in prediction behaviour right away to stop any customer impacts by fixing issues at their start.

The financial sector experienced many data breach events because companies failed to implement DevSecOps in their Artificial Intelligence development. Attackers exploited a lending system's machine learning functions because its access controls were weak enough for them to extract training data from it. A significant data leak occurred when API services related to the credit scoring engine remained unprotected. The analyzed breaches show where security failures usually happen such as when endpoint defenses are missing and no deployment controls exist (Jain, Gyanchandani, & Khare, 2016).

Organizations protect themselves by matching their activities to new DevSecOps guidelines for AI/ML systems. Organizations should develop threat analytics systems, encrypt data throughout processes, and scan both software and models to check for weaknesses plus record all model outputs for legal verification and tracking. They require regular checks to find problems that slowly damage model reliability.

Financial companies use zero-trust architectures as they expand their AI technology base. A system built under this model lacks complete trust in all elements and must validate them throughout all layers. Financial institutions can create reliable AI security by pairing zero trust architectures with special AI security features (Pathak & Bhandari, 2018).

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

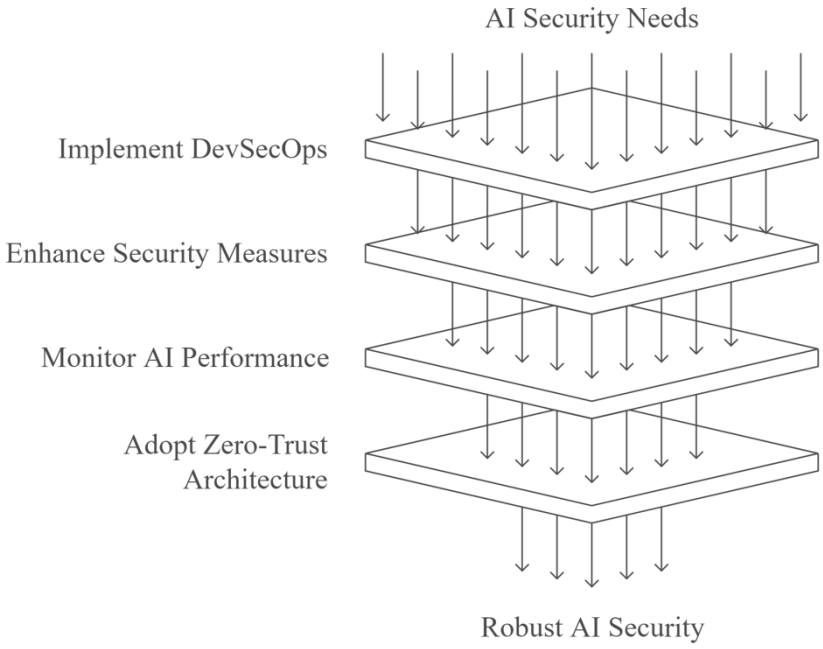

Figure 2: Enhancing AI Security in Finance

6. CONCLUSION

The implementation of security at each level of model development stands as the most vital point since financial institutions now heavily depend on AI and machine learning for critical operational choices. The implementation of DevSecOps security practices across the entire data ingestion to deployment spectrum enables banks and insurance firms to develop AI models which demonstrate power while being efficient along with trustworthy security features and regulatory compliance and design resilience against upcoming threats. Financial AI models carry inherent high-risk due to both the sensitive nature of utilized data along with the considerable impact from their generated decisions. Unwarranted model bias combined with data breach incidents or unauthorized system access leads to extensive financial losses and severe damage to brand reputation for financial organizations. The financial sector requires AI/ML security and model risk management as fundamental elements of their AI strategy. DevSecOps implements security as an ongoing automated collaborative practice between teams through its approach which eliminates security treatment as an afterthought. The security mechanisms embedded through DevSecOps help organizations identify threats proactively while ensuring regulatory compliance standards and constructing models that resist cyberattacks and regulatory examinations. Organizations following DevSecOps deployments will find better success in large-scale and ethical innovation due to increasing expectations from regulators along with customers and stakeholders regarding data governance and ethical AI standards.

Financial companies integrating DevSecOps into their financial AI systems gain a market advantage through this operational practice. Financial institutions achieve safer and accelerated deployment of smarter models through DevSecOps which drives long-term success for AI applications in banking along with insurance functions.

REFERENCES

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[1] Alimohammadlou, M., & Bonyani, A. (2017). A novel hybrid MCDM model for financial performance evaluation in Iran's food industry. Accounting and Financial Control, 1(2), 38–45. https://doi.org/10.21511/afc.01(2).2017.05
[2] Bennett, D. E. (2017). Governance and organizational requirements for effective model risk management. Journal of Risk Model Validation, 11(4), 97–116. https://doi.org/10.21314/JRMV.2017.188
[3] Cobb, S. (2016). Data privacy and data protection: US law and legislation. Eset, (April), 1–16. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacy-legislation-white-paper.pdf
[4] Crespo, I., Kumar, P., & Noteboom, P. (2017). The evolution of model risk management. McKinsy Global Institute, 1–8.
[5] Dagoumas, A. S., Koltsaklis, N. E., & Panapakidis, I. P. (2017). An integrated model for risk management in electricity trade. Energy, 124, 350–363. https://doi.org/10.1016/j.energy.2017.02.064
[6] Dash, S. (2018). An Efficient AI Model for Financial Market Prediction Optimized by SVR. International Journal for Research in Applied Science and Engineering Technology, 6(5), 1884–1889. https://doi.org/10.22214/ijraset.2018.5307
[7] De Almeida, A. T., Alencar, M. H., Garcez, T. V., & Ferreira, R. J. P. (2017, April 1). A systematic literature review of multicriteria and multi-objective models applied in risk management. IMA Journal of Management Mathematics. Oxford University Press. https://doi.org/10.1093/imaman/dpw021
[8] Díaz, J., Pérez, J. E., Lopez-Peña, M. A., Mena, G. A., & Yagüe, A. (2019). Self-service cybersecurity monitoring as enabler for DevSecops. IEEE Access, 7, 100283–100295. https://doi.org/10.1109/ACCESS.2019.2930000
[9] Financial Stability Board. (2017). Artificial Intelligence and Machine Learning in Financial Services - Market Developments and Financial Stability Implications. Financial Stability Board, (November), 45. Retrieved from http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/
[10] Holzinger, A., Kieseberg, P., Weippl, E., & Tjoa, A. M. (2018). Current advances, trends and challenges of machine learning and knowledge extraction: From machine learning to explainable AI. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 11015 LNCS, pp. 1–8). Springer Verlag. https://doi.org/10.1007/978-3-319-99740-7_1
[11] Jain, M. S. (2017). ARTIFICIAL INTELLIGENCE-THE ENGINE DRIVING THE NEXT WAVE OF TRANSFORMATION IN BUSINESS. Modi Institute of Management, 22(23), 215–219.
[12] Jain, P., Gyanchandani, M., & Khare, N. (2016). Big data privacy: a technological perspective and review. Journal of Big Data, 3(1). https://doi.org/10.1186/s40537-016-0059-y
[13] Kazi, Z., & Saniora, D. (2019). A new project management tool based on devsecops. In Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019 (pp. 239–243). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CSCI49370.2019.00049
[14] Kumar, D., Taylor, G. W., & Wong, A. (2017). Opening the Black Box of Financial AI with CLEAR-Trade: A CLass-Enhanced Attentive Response Approach for Explaining and Visualizing Deep Learning-Driven Stock Market Prediction. Journal of Computational Vision and Imaging Systems, 3(1). https://doi.org/10.15353/vsnl.v3i1.166
[15] Mai, J. E. (2016). Big data privacy: The datafication of personal information. Information Society, 32(3), 192–199. https://doi.org/10.1080/01972243.2016.1153010
[16] Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G., & Guo, S. (2016). Protection of big data privacy. IEEE Access, 4, 1821–1834. https://doi.org/10.1109/ACCESS.2016.2558446
[17] Pathak, N., & Bhandari, A. (2018). IoT, AI, and Blockchain for .NET. IoT, AI, and Blockchain for .NET. Apress. https://doi.org/10.1007/978-1-4842-3709-0
[18] Prates, L., Faustino, J., Silva, M., & Pereira, R. (2019). DevSecOps metrics. In Lecture Notes in Business Information Processing (Vol. 359, pp. 77–90). Springer Verlag. https://doi.org/10.1007/978-3-030-29608-7_7

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

[19] Rahul, S. P. K. M. M. N. (2019). Implementation of DevSecOps using Open-Source tools. International Journal of Advance Research, 5(3), 1050–1051. Retrieved from www.IJARIIT.com
[20] Sajid, A., & Abbas, H. (2016). Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and Future Challenges. Journal of Medical Systems, 40(6). https://doi.org/10.1007/s10916-016-0509-2
[21] Soria-Comas, J., & Domingo-Ferrer, J. (2016). Big Data Privacy: Challenges to Privacy Principles and Models. Data Science and Engineering, 1(1), 21–28. https://doi.org/10.1007/s41019-015-0001-x
[22] Svenmarck, P., Luotsinen, L., Nilsson, M., & Schubert, J. (2018). Possibilities and Challenges for Artificial Intelligence in Military Applications. In Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting (pp. 1–16).
[23] Tiwari, T., Tiwari, T., & Tiwari, S. (2018). How Artificial Intelligence, Machine Learning and Deep Learning are Radically Different? International Journal of Advanced Research in Computer Science and Software Engineering, 8(2), 1. https://doi.org/10.23956/ijarcsse.v8i2.569
[24] Tomas, N., Li, J., & Huang, H. (2019). An empirical study on culture, automation, measurement, and sharing of DevSecOps. In 2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CyberSecPODS.2019.8884935
[25] van Biljon, L., & Haasbroek, L. J. (2017). A practical maturity assessment method for model risk management in banks. Journal of Risk Model Validation, 11(4), 79–95. https://doi.org/10.21314/JRMV.2017.171
[26] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security? IEEE Signal Processing Magazine, 35(5), 41–49. https://doi.org/10.1109/MSP.2018.2825478