Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Understanding AI-Powered Risk Scoring in Identity Systems

Gowtham Kukkadapu
Independent Researcher, USA

ARTICLE INFO

Received: 06 Nov 2025
Revised: 18 Dec 2025
Accepted: 26 Dec 2025

ABSTRACT

Present-day identity safety architectures face mounting demanding situations from credential-based intrusions concentrated on the authentication infrastructure. Traditional rule-based authentication mechanisms depend on static policies and predetermined thresholds. Such mechanisms fail to distinguish legitimate users exhibiting unusual behavior from malicious actors employing stolen credentials. AI-powered risk scoring offers a transformative alternative through continuous behavioral modeling and dynamic threat assessment. Machine learning algorithms process authentication telemetry streams to construct individualized behavioral profiles. Feature extraction techniques transform raw interaction data into meaningful indicators suitable for anomaly detection. Unsupervised learning architectures, including autoencoders and deep belief networks, identify deviations from established baselines without requiring labeled threat examples. Ensemble methods aggregate predictions from diverse model architectures to enhance detection robustness. Risk scores operate on continuous scales, enabling graduated authentication responses proportional to detected threat likelihood. Policy engines map score ranges to specific authentication actions, ranging from transparent approval through step-up verification to complete access denial. Concept drift adaptation mechanisms ensure model effectiveness as user behaviors evolve. The mixing of adaptive threat engines with authentication frameworks enables security controls conscious of evolving hazard landscapes, even as retaining a satisfactory user experience.

Keywords: Risk-Based Authentication, Behavioral Analytics, Anomaly Detection, Machine Learning Security, Adaptive Authentication, Identity Threat Detection

Introduction

Identity systems constitute the primary attack surface in modern enterprise environments. Credential-based intrusions constitute a foremost chance vector across organizational boundaries. Information breach incidents have escalated throughout multiple geographic regions and industry sectors. The worldwide distribution of such incidents reflects systemic vulnerabilities in authentication infrastructure in preference to isolated screw-ups [1]. Compromised credentials permit attackers to masquerade as valid customers. This technique permits adversaries to pass perimeter defenses absolutely. The exploitation of identity mechanisms has become a preferred attack methodology due to reduced detection probability compared to technical vulnerability exploitation [1].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Conventional authentication mechanisms employ static policies. Fixed password requirements govern access decisions. Predetermined access schedules restrict login availability. Binary allow-deny rules evaluate each request independently. Such processes show insufficient opposition to state-of-the-art adversaries. Attackers reap legitimate credentials through phishing campaigns. Credential stuffing assaults leverage previously breached password databases. Social engineering manipulates humans to extract authentication records. Rule-based frameworks operate on predetermined thresholds established during initial configuration. These thresholds remain fundamentally unchanged regardless of evolving threat landscapes.

The taxonomy of computer security research identifies authentication and access control as foundational security domains [2]. Early security frameworks recognized the distinction between static verification and dynamic assessment approaches [2]. Static policies evaluate only discrete attributes such as password correctness. Source IP address ranges undergo binary matching. Time-of-day restrictions apply uniform constraints. Such mechanisms cannot contextualize access requests within broader behavioral patterns. The fundamental limitation lies in distinguishing legitimate users exhibiting unusual behavior from malicious actors employing stolen credentials.

Credential theft techniques have achieved substantial sophistication. Adversaries conduct reconnaissance sufficient to replicate expected access patterns. Phishing campaigns incorporate organizational context. Targeted individuals receive tailored pretexts yielding credentials along with behavioral intelligence. Typical access times become known to attackers. Frequently utilized applications are identified. Network locations are documented. Consequently, attackers armed with stolen credentials may present authentication requests satisfying every static policy criterion. Such requests nonetheless represent unauthorized access requiring detection through alternative means.

Recognition of static policy limitations has driven authentication architecture evolution. Risk-adaptive frameworks evaluate contextual signals dynamically. Fixed rules no longer apply uniformly across all access attempts. AI-powered risk scoring addresses authentication challenges through continuous behavioral modeling. Machine learning algorithms process authentication telemetry streams. Individualized behavioral profiles emerge from sustained observation. Statistical baselines establish expected patterns against which subsequent access requests undergo evaluation. Session-specific risk scores reflect compromise probability based on observed characteristics. Graduated authentication responses range from transparent approval through step-up verification to complete access denial.

This article provides a technical examination of risk scoring mechanisms. The analysis addresses contextual signal processing approaches. Feature weighting methodologies receive detailed treatment. The synthesis of multiple indicators into authentication decisions forms the central focus.

Related Work and Technical Framework

Prior contributions in authentication security have addressed credential protection through multi-factor verification schemes and policy-based access control mechanisms. Behavioral biometrics literature has established foundational techniques for user identification through typing patterns and interaction dynamics. Network anomaly detection scholarship has demonstrated machine learning effectiveness for identifying malicious traffic patterns. However, existing literature lacks a comprehensive treatment of integrated risk scoring architectures combining behavioral signals, device fingerprinting, and environmental context within unified authentication frameworks.

The article advances a technical framework positioning continuous behavioral modeling as the foundation for adaptive authentication decisions. The central argument maintains that static rule-

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

based authentication cannot address sophisticated credential theft attacks. Dynamic risk assessment through machine learning offers superior detection capability for novel threats. The framework integrates multiple signal categories, including temporal access patterns, device telemetry, and geographic indicators. Feature engineering transforms raw authentication telemetry into structured representations suitable for anomaly detection algorithms. Ensemble model architectures aggregate diverse classifier outputs for enhanced robustness. The contribution establishes conceptual foundations for understanding risk engine operation within modern identity architectures. Graduated authentication responses enable security controls proportional to assessed threat likelihood. Concept drift adaptation ensures sustained model effectiveness despite evolving behavioral patterns across user populations.

Behavioral Signal Extraction and Feature Engineering

User Activity Pattern Analysis

Risk scoring engines ingest continuous streams of user interaction data. Behavioral baselines emerge from sustained observation of authentication telemetry. Temporal access characteristics form a foundational signal category. Typical login times establish expected access windows. Session duration distributions reveal normal engagement patterns. Activity frequency within applications indicates routine operational behavior. Machine learning methodologies have become essential for detecting anomalous patterns within network and user activity streams [3]. Traditional signature-based approaches cannot identify novel attack patterns. Learning-based methods offer adaptive detection capabilities that evolve with changing behavioral landscapes [3].

Feature extraction algorithms identify recurring sequences in user interactions. Navigation paths through application interfaces follow predictable patterns during legitimate sessions. Document access behaviors demonstrate consistency across similar work contexts. Transaction sequences exhibit regularity in timing and composition. Feature representation constitutes a critical component of anomaly detection system design [3]. Raw telemetry data requires transformation into structured feature vectors. Statistical features capture distributional properties of behavioral signals. Temporal features encode time-series characteristics of user activities. The selection of appropriate features directly influences detection accuracy and computational efficiency [3].

Individual user signatures emerge from the combination of multiple behavioral dimensions. Authentication risk models evaluate new sessions against established signatures. Deviation magnitude determines risk contribution from behavioral analysis components. Supervised learning approaches require labeled datasets distinguishing normal from anomalous behavior. Unsupervised methods detect deviations without prior attack examples [3]. Semi-supervised techniques leverage limited labeled data alongside abundant unlabeled observations. Deep learning architectures have demonstrated particular effectiveness for complex behavioral pattern recognition [3].

Device and Environmental Context

Risk models incorporate device-level telemetry beyond behavioral signals. Operating system configurations provide baseline device characterization. Browser characteristics offer additional differentiation capability. Browser fingerprinting enables device identification through the collection of configuration attributes [4]. The uniqueness of browser fingerprints varies across user populations. Demographic factors influence fingerprint distinctiveness in measurable ways [4]. Different population segments exhibit varying levels of fingerprint uniqueness based on device usage patterns and configuration preferences.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Screen resolution contributes identification signal strength. Installed plugins and extensions provide differentiating characteristics. Canvas rendering produces device-specific outputs useful for identification. WebGL parameters reveal graphics hardware configurations. Timezone settings and language preferences add contextual dimensions. The combination of multiple attributes creates composite fingerprints with enhanced uniqueness [4]. Individual attributes may appear common across many users. Attribute combinations produce substantially more distinctive identifiers. Browser fingerprinting effectiveness depends on the diversity of configurations within the target population [4].

Environmental factors provide additional contextual dimensions for risk calculation. Network topology reveals access pathway characteristics. Connection types distinguish corporate network access from public infrastructure. Geographic coordinates establish physical location context. Location velocity analysis detects impossible travel scenarios. Network reputation databases inform risk scoring with historical threat intelligence. The integration of device fingerprinting with behavioral analysis strengthens identity verification beyond credential validation alone.

Signal Category	Feature Type	Description
Temporal Access	Login Timing	Expected access windows based on historical patterns
	Session Duration	Normal engagement period distributions
	Activity Frequency	Routine operational behavior within applications
Behavioral Pattern	Navigation Paths	Recurring sequences through application interfaces
	Document Access	Consistency in file interaction behaviors
	Transaction Sequences	Regularity in timing and composition
Device Telemetry	Browser Configuration	Screen resolution, plugins, fonts, timezone
	Hardware Attributes	Operating system, graphics parameters
Environmental Context	Geographic Location	Physical access location coordinates
	Network Topology	Connection type and access pathway characteristics

Table 1. Graduated Authentication Actions Based on Risk Assessment Levels [3, 4].

Machine Learning Architectures for Risk Computation

Anomaly Detection Frameworks

Risk scoring systems employ unsupervised learning approaches to identify deviations from established baselines. Labeled threat examples remain scarce in operational environments. Attack patterns evolve continuously. Historical labels prove insufficient for detecting emerging threats. Deep learning techniques have transformed anomaly detection capabilities across multiple domains [5]. Neural network architectures learn hierarchical feature representations automatically. Manual feature

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

engineering becomes unnecessary with deep learning approaches. The ability to extract complex patterns from raw data distinguishes deep learning from traditional methods [5].

Autoencoders constitute a foundational architecture for anomaly detection applications. The encoder network compresses input data into lower-dimensional latent representations. The decoder network reconstructs original inputs from compressed encodings [5]. Training occurs exclusively on normal behavioral samples. The network learns to minimize reconstruction error for legitimate patterns. Anomalous inputs produce elevated reconstruction errors due to unfamiliar characteristics. Variational autoencoders extend basic autoencoder architectures with probabilistic frameworks [5]. Latent representations follow specified probability distributions. This probabilistic formulation enables generative capabilities alongside anomaly detection.

Deep belief networks offer alternative architectures for unsupervised feature learning. Restricted Boltzmann machines form the building blocks of deep belief network construction [5]. Layer-wise pretraining establishes initial network parameters. Fine-tuning optimizes the complete network for specific detection objectives. Recurrent neural networks capture temporal dependencies in sequential information. Long short-term memory architectures address vanishing gradient challenges in extended sequences [5]. Convolutional neural networks excel at detecting spatial patterns within structured inputs. Hybrid architectures combine multiple network types for comprehensive pattern analysis.

Ensemble Model Integration

Production risk engines combine multiple algorithmic approaches to enhance detection robustness. Individual models exhibit distinct strengths across different threat categories. Ensemble methods aggregate predictions from diverse model architectures to improve overall accuracy [6]. The combination of multiple classifiers typically outperforms individual constituent models. Behavioral models contribute to user activity pattern analysis. Device reputation systems evaluate endpoint trustworthiness. Network analysis components assess connection characteristics.

Ensemble classifier construction involves strategic selection of base learners [6]. Diversity among constituent models enhances ensemble effectiveness. Homogeneous ensembles combine multiple instances of identical algorithms trained on varied data subsets. Heterogeneous ensembles integrate fundamentally different algorithmic approaches. The integration of diverse classification methods strengthens predictive performance [6]. Base classifiers may include decision trees, support vector machines, neural networks, and probabilistic models.

Voting mechanisms aggregate individual classifier outputs into final predictions [6]. Hard voting selects the class receiving majority support from constituent classifiers. Soft voting averages probability estimates across all base models. Weighted voting assigns differential influence based on classifier reliability. Historical accuracy within specific contexts informs weight allocation decisions. Models demonstrating superior performance receive elevated contribution weights. Dynamic weighting adjusts allocations based on recent performance observations. The strategic combination of multiple detection perspectives reduces false positive rates. Ensemble approaches provide resilience against adversarial manipulation targeting individual model vulnerabilities.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Architecture Type	Learning Approach	Detection Mechanism
Autoencoder	Unsupervised	Elevated reconstruction error for anomalous inputs
Variational Autoencoder	Unsupervised	Probabilistic latent representations with generative capability
Deep Belief Network	Unsupervised	Layer-wise pretraining with restricted Boltzmann machines
Recurrent Neural Network	Supervised/Unsupervised	Temporal dependency capture in sequential data
Long Short-Term Memory	Supervised/Unsupervised	Extended sequence modeling addressing gradient challenges
Convolutional Neural Network	Supervised	Spatial pattern detection in structured inputs
Ensemble Classifier	Hybrid	Aggregated predictions from diverse base learners

Table 2. Machine Learning Model Types and Detection Mechanisms [5, 6].

Risk Score Integration with Authentication Decisions

The computed risk score serves as input to policy engines that determine appropriate authentication responses. Policy engines evaluate risk scores against configurable thresholds. Different threshold ranges trigger distinct authentication workflows. Risk-based authentication has emerged as a practical approach deployed by major online services [7]. The core principle involves collecting contextual features during login attempts. These features undergo analysis to determine session risk levels. Authentication requirements adjust dynamically based on computed risk assessments [7].

Low-risk sessions may proceed with minimal friction. Risk-based authentication systems analyze multiple feature categories to establish session legitimacy [7]. IP address characteristics provide network-level context. Device fingerprinting captures browser and hardware attributes. Geographic location establishes physical access context. Login history comparison identifies deviations from established patterns [7]. Sessions matching historical behavioral profiles receive expedited authentication. The reduction of authentication burden during low-risk scenarios improves user experience significantly.

Elevated scores trigger step-up authentication requirements. Multi-factor authentication provides additional identity assurance when risk indicators warrant scrutiny. Authentication factors fall into three fundamental categories [8]. Expertise elements consist of passwords, pins, and safety questions. Possession factors encompass hardware tokens, smart cards, and mobile devices. Inherence factors leverage biometric characteristics unique to individual users [8]. The combination of multiple factor types strengthens authentication assurance substantially.

Biometric authentication has gained prominence as a step-up verification mechanism [8]. Physiological biometrics consist of fingerprint recognition, facial recognition, and iris scanning. Behavioral biometrics analyzes typing patterns, gait characteristics, and voice features. Continuous authentication extends verification beyond initial login events [8]. Ongoing behavioral monitoring

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

detects session compromise after initial authentication succeeds. This approach addresses session hijacking threats that bypass point-in-time verification.

Sessions exhibiting extreme risk indicators may face access restrictions or complete blocking. Administrative review processes evaluate blocked sessions for potential false positives. Risk-based authentication systems must balance security enhancement against usability degradation [7]. Overly aggressive blocking generates excessive false positives, frustrating legitimate users. Insufficient sensitivity permits unauthorized access despite available contextual signals.

Risk scores operate on continuous scales rather than binary classifications. Continuous scoring enables graduated responses proportional to detected threat likelihood. Binary allow-deny decisions cannot express nuanced risk assessments. The granularity of continuous scoring supports flexible policy configuration. Security architects define threshold ranges mapping to specific authentication actions. Slightly elevated scores may require additional verification steps. Moderately elevated scores demand multi-factor authentication completion. Severely elevated scores necessitate administrative intervention.

This granularity allows security architects to balance protection strength against user experience degradation. Organizational risk tolerance influences threshold configuration decisions. Feature selection significantly impacts risk-based authentication effectiveness [7]. The weighting of individual features requires empirical calibration. Continuous refinement based on operational outcomes optimizes detection accuracy over time. The integration of risk scoring with adaptive authentication creates security frameworks responding dynamically to evolving threat landscapes.

Risk Level	Score Range	Authentication Response	Verification Requirements
Low	Baseline	Transparent Approval	Standard credential verification
Slightly Elevated	Above Baseline	Email Verification	Additional confirmation step
Moderate	Mid-Range	Multi-Factor Authentication	Knowledge or possession factor
High	Upper Range	Biometric Verification	Physiological or behavioral factor
Severe	Critical	Administrative Review	Manual intervention required
Extreme	Maximum	Complete Blocking	Access denial pending investigation

Table 3. Graduated Authentication Actions Based on Risk Assessment Levels [7, 8].

Adaptive Learning and Model Evolution

Continuous Baseline Refinement

Effective risk scoring requires ongoing model adaptation as legitimate user behaviors evolve. Static models trained on historical data degrade over time. The statistical distribution of input data shifts in production environments. Concept drift occurs when the relationship between input features and target variables changes [9]. This phenomenon poses significant challenges for deployed machine learning systems. Models optimized for historical distributions become increasingly misaligned with current data characteristics [9].

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Users change devices frequently in modern computing environments. Travel patterns fluctuate based on project requirements. Work schedule modifications alter expected access timing distributions. Without continuous learning mechanisms, static models would increasingly generate false positives as behavioral drift accumulates. Deep learning frameworks offer specific advantages for concept drift adaptation [9]. Neural network architectures can incorporate new knowledge through incremental parameter updates. Transfer learning techniques leverage previously learned representations for rapid adaptation.

Concept drift manifests in multiple forms requiring distinct adaptation strategies [9]. Sudden drift involves abrupt distribution changes occurring instantaneously. Gradual drift represents slow transitions between distributions over extended periods. Incremental drift accumulates through small sequential changes. Recurring drift involves cyclical patterns returning to previously observed distributions [9]. Each drift type demands appropriate detection and adaptation mechanisms.

Active adaptation strategies explicitly detect drift before triggering model updates [9]. Passive adaptation strategies continuously update models regardless of detected drift. Hybrid approaches combine drift detection with continuous learning mechanisms. The selection of appropriate adaptation strategies depends on application requirements and computational constraints. Deep learning models benefit from replay-based methods that retain representative historical samples [9]. Regularization techniques prevent catastrophic forgetting throughout incremental updates.

Threat Landscape Responsiveness

AI-driven systems demonstrate inherent advantages in responding to novel attack methodologies. Intrusion detection systems employ two fundamental detection approaches [10]. Signature-based detection matches observed patterns against known attack signatures. Anomaly-based detection identifies deviations from established normal behavior profiles [10]. Each approach exhibits distinct strengths and limitations in operational environments.

Signature-based methods achieve high accuracy for known attack patterns. False positive rates remain low when signatures precisely characterize threats. However, novel attacks evade detection until signatures receive updates [10]. The time gap between attack emergence and signature availability creates vulnerability windows. Zero-day attacks exploit this fundamental limitation extensively.

Anomaly-based detection identifies statistical deviations regardless of attack specifics [10]. Machine learning algorithms characterize normal behavioral distributions during training phases. Observations falling outside learned boundaries trigger alerts without requiring explicit attack knowledge. This approach enables the detection of previously unseen attack patterns. Data mining techniques extract meaningful patterns from authentication telemetry [10]. Classification algorithms assign risk categories to observed sessions. Clustering methods group similar behavioral patterns for baseline establishment.

Feature selection significantly impacts detection system effectiveness [10]. Relevant features enhance discrimination between legitimate and malicious sessions. Irrelevant features introduce noise, degrading classification accuracy. The integration of multiple machine learning methods strengthens detection robustness against diverse attack methodologies.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Drift Type	Characteristics	Adaptation Strategy	Update Mechanism
Sudden Drift	Abrupt distribution change	Active detection with immediate retraining	Complete model refresh
Gradual Drift	Slow transition between distributions	Sliding window techniques	Progressive parameter adjustment
Incremental Drift	Small sequential accumulating changes	Continuous passive updates	Incremental learning
Recurring Drift	Cyclical return to previous distributions	Ensemble with temporal diversity	Multi-model retention
General Adaptation	All drift types	Replay-based methods	Historical sample retention
Stability Preservation	Preventing catastrophic forgetting	Regularization techniques	Constrained parameter updates

Table 4. Model Evolution Mechanisms Addressing Behavioral Distribution Changes [9, 10].

Conclusion

AI-powered risk scoring fundamentally transforms identity security capabilities beyond traditional static authentication paradigms. Credential-based attacks continue dominating threat landscapes as adversaries recognize authentication infrastructure as the path of least resistance. Static policies applying identical requirements regardless of contextual factors cannot address sophisticated adversaries employing stolen credentials with behavioral intelligence. Dynamic risk assessment through machine learning enables nuanced authentication decisions reflecting actual threat probability rather than predetermined threshold violations. Behavioral signal extraction captures temporal access patterns, navigation sequences, and transaction characteristics defining individual user signatures. Device fingerprinting leverages browser configurations and hardware attributes for endpoint identification across sessions. Deep learning architectures learn hierarchical feature representations automatically without manual engineering requirements. Autoencoder networks identify anomalous sessions through elevated reconstruction errors when inputs deviate from learned normal patterns. Ensemble classifier integration combines diverse algorithmic perspectives for enhanced detection robustness against varied attack methodologies. Continuous baseline refinement through concept drift adaptation maintains model accuracy as legitimate behavioral patterns evolve. Graduated authentication responses balance security enhancement against usability degradation through configurable threshold ranges. The strategic deployment of risk-adaptive authentication creates identity frameworks responding dynamically to emerging threats while minimizing friction for legitimate access attempts across enterprise environments.

References

[1] Gabriel Arquelau Pimenta Rodrigues et al., "Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review," MDPI, 2024. [Online]. Available: https://www.mdpi.com/2306-5729/9/2/27

[2] Catherine Meadows, "An Outline of a Taxonomy of Computer Security Research and Development," ACM, 1993. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/283751.283770

[3] SONG WANG et al., "Machine Learning in Network Anomaly Detection: A Survey," IEEE Access, 2021. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9610045

[4] Alex Berke et al., "How Unique is Whose Web Browser? The Role of Demographics in Browser Fingerprinting among US Users" arXiv, 2024. [Online]. Available: https://arxiv.org/pdf/2410.06954

[5] Raghavendra Chalapathy and Sanjay Chawla, "DEEP LEARNING FOR ANOMALY DETECTION: A SURVEY," arXiv, 2019. [Online]. Available: https://arxiv.org/pdf/1901.03407

[6] Prabh Deep Singh et al., "A Novel Ensemble-based Classifier for Detecting the COVID-19 Disease for Infected Patients," Springer, 2021. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s10796-021-10132-w.pdf

[7] Stephan Wiefling et al., "Is This Really You? An Empirical Study on Risk-Based Authentication Applied in the Wild," arXiv, 2020. [Online]. Available: https://arxiv.org/pdf/2003.07622

[8] SYED W. SHAH AND SALIL S. KANHERE, "Recent Trends in User Authentication - A Survey," IEEE Access, 2019. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8784263

[9] Qiuyan Xiang et al., "Concept Drift Adaptation Methods under the Deep Learning Framework: A Literature Review," MDPI, 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/11/6515

[10] Anna L. Buczak et al., "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, 2016. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7307098