Index

Note: Page numbers followed by "*b*," "*f*," and "*t*" refer to boxes, figures, and tables, respectively.

A

Abuse detection, 293
Access control, 382
  mechanisms, 40
  scheme, 319–321
  types of, 382
Access Point Name (APN), 72
Accountability, 255, 261, 480
Account model, 189
Account takeover attacks, 290–291
Accuracy, 330, 425
Adaptive access controls, 375
Adaptive response mechanism, 297–298
Adaptive security architectures, 374–375
Adaptive thresholds, 192
Administrator.wab file, 354–355
ADMs. *See* Adversarial defense mechanisms (ADMs)
Advanced anomaly detection systems, 289
Advanced Encryption Standard (AES), 5
Advanced persistent threats (APTs), 1–2, 348
Adversarial defense mechanisms (ADMs), 63–64, 66*t*
  data collection, 69–71
  data preprocessing, 72
    encoding categorical variables, 72
    identification of categorical columns and normalization, 72
    splitting data, 72
  evaluation metrics, 74–77
    prediction and metrics, 75
    receiver operating characteristic curve analysis, 75
    visualizations, 76–77
  header data for adversarial datasets, 71*t*
  limitation of, 81
  model selection and hyperparameters tuning, 73–74
  performance metrics, 78–81
    classification report, 78
    comparison of numeric results based on existing works, 81
    confusion matrix, 79, 79*f*
    receiver operating characteristic curve analysis, 80
Adversarial defenses, 14–15
Adversarial machine learning attacks, 290
Adversarial training, 14
Aggregation process, 203
Aggregation servers, 265
Agriculture, 325
AI. *See* Artificial intelligence (AI)
AI-driven security systems, 433
AI-enhanced security, 27
AI-powered cyber attacks, 434
AI-powered threat analysis, 289
AI-powered trust mechanisms, 460
Algorithmic fairness, 441
Amazon web service, 89, 360–361
Anomaly detection techniques, 105
Apple, 127
Application programming interfaces (API), 38, 87
  security, 39
APTs. *See* Advanced persistent threats (APTs)
Architectural design principles, 30–32
  defense in depth, 31
  least privilege, 31–32
  security by design, 30
Area under the curve (AUC), 75
Artificial intelligence (AI), 1–3, 13–14, 24, 275, 339, 360
  driven compliance monitoring, 502–503
  integration, 56
Asia-Pacific regions, 490–491
Asynchronous streaming protocol, 266–267
Atomic swaps, 186
Attack Category (attack_cat), 408
Attentional generative adversarial network (AttnGAN), 65–68
Attribute-based access control (ABAC), 324, 382
Auditing, 379
Automated incident response, 289
Automated response systems, 347
Automation, 293, 375
Autonomous vehicles, 292, 325, 362, 432

B

Backdoor detection technique, 224–225
Bandwidth optimization, 2
Batch normalization, 322–323
Behavioral analysis, 17, 298
Behavioral analytics, 375

Behavioral anomaly detection, 378
Behavioral-based detection techniques, 341, 346
Bias, 255, 441
Bias-reducing algorithms, 255
Bidirectional long short-term memory (BiLSTM) networks, 108
Big data, 360
Bijection, 301
Binary classification, 112–113
Binary Functionality Description Language, 225
BinGold, 226
Binomial distribution, 132–133
Biometric-based access control mechanism, 318, 329
  application areas of edge computing, 325
  biometric-based authentication techniques employed in edge computing, 324
  edge computing authentication techniques, 328–331
  for edge resources and services, 321–323, 321*t*
  popular authorization mechanisms used in edge computing, 323–324
  software and hardware configuration of, 330–331
  traditional access control mechanisms for edge resources and services, 319–321
Biometric sensors, 331
Biometric Software Development Kit (SDK), 331
Bitcoin, 179, 186
Blockchain technology, 4–5, 13, 129, 173, 178–182, 360
  for access control, 382
  architecture, 366*f*
  decentralized and immutable characteristics of, 389
  in edge computing, 382–383
    healthcare systems, 383
    IoT networks, 383
    smart cities, 383
  and edge computing integration, 363–364
    addressing security, scalability, and efficiency issues, 363
    handling data integrity and security issues, 364
    for network edge services, 364
    overcoming integration challenges, 364
  emergence of edge computing, 362–363
  energy-efficient blockchain technologies, 388
  for enhancing data integrity, 380
  ensuring trust with, 380–382
  evolution of cloud computing, 360–361
  future scopes and research directions, 388
  innovations in decentralized computing, 389
  integration, 27
  key characteristics of, 367
  overview of, 360
  scalability issues and solutions, 388
  systems, 176
    consensus mechanisms and implications for scalability, 179–180
    core principles of, 178–179
    opportunities and challenges, 180*f*, 181–182
  technological integration, 383–387
    designing blockchain-enabled edge computing architectures, 385–387
    integration challenges, 384
    limitations of blockchain and edge computing integration, 384–385
    solutions and best practices, 384
  types of, 367–368, 368*f*
Block hash, 200, 200*f*
Block hash verification performance, 207–208
  next block producer hash verification performance, 213–214
  proof aggregation and final block verification performance, 215–216
  real block analysis, 207–208
  signature verification performance, 209–211
  synthetic data analysis, 207
  validator key and stake verification performance, 211–213
Block header, 365
Block number, 365
Blocks, 365
Block search placement algorithm, 162–163
Bloom filter (BF), 145
Bug detection system, 226
Bulletproofs, 184
Business-to-business (B2B) scenario, 305
Byzantine fault tolerance (BFT), 179, 380

C
California Consumer Privacy Act (CCPA), United States, 435–436, 455, 473
California Privacy Rights Act, 473
Capability-based access control (CapBAC), 382
Carlini and Wagner (CW) Attack, 69–72, 82
C&C server. *See* Command and control (C&C) server
CDNs. *See* Content delivery networks (CDNs)
Cell Identity (CI), 72
Celo, 188
Census datasets, 134, 137
Centers for Disease Control and Prevention (CDC), 143
Central processing unit (CPU), 89
CereCrow.eUw, 352–353
Chunk, 190
Chunk-only producers, 190
Chunk producers, 189
Circuit generation, 196
Client selection, 252

Cloud computing, 86
  architecture, 361*f*
  evolution of, 360–361
CloudSim environment, 157
Code injection, 343–344
Code obfuscation, 341
Codomain B, 301*f*
Collaboration barriers, 295–296
Collusion attacks, 129
Command and control (C&C) server, 338, 341–342
Common Vulnerabilities and Exposures (CVE) database, 400
Communication protocols, 262, 266–267
Community-based security models, 439–440
Community-driven threat monitoring, 452
Compatibility, 194
Composite mapping, 302*f*
Confidential data exposure, 370
Confidentiality, 260–261
Configuration management, 41
Confusion matrix, 79, 79*f*, 417–419, 419*f*
  linear support vector machine, 417
  polynomial support vector machine, 419
  radial basis function support vector machine, 418
  sigmoid support vector machine, 418–419, 421*f*
Con-Pi framework, 98
Consensus mechanisms, 179–180, 189, 319–321
Consent management, 479
Consortium blockchain, 368
Containers, 85, 87–89
Container security, 40, 379
Content delivery networks (CDNs), 6
Continuous monitoring, 375, 379
Convolutional neural networks (CNNs), 108
Coordination mechanisms, 36
Core security requirements, 29–30
  availability assurance, 30
  confidentiality guarantees, 29, 29*f*
  integrity preservation, 29–30
COVID-19 pandemic, 123–124
Credential stuffing attacks, 290–291
Cross-border data governance, 503, 507
Cryptographic primitives, 205
Cryptographic protocols, 265–266
Cryptographic techniques, 256–257, 365
Cumulative distribution function (CDF), 131
Curve25519, 200–201
Cyberattacks, 221–222, 375, 431–432
  social and ethical implications of, 433
Cybercriminals, 401, 432–433
Cyber edge computing systems
  data protection and privacy regulations in, 470–483
    challenges in regulatory compliance for, 479–481
    emerging strategies for regulatory compliance in edge computing, 481–483
    global data protection laws and impact on edge computing, 473–479
  emerging regulatory frameworks and policy initiatives, 490–502
  liability and accountability in edge computing, 483–490
    case studies on accountability in edge computing incidents, 486–488
    complex liability challenges, 484–486
    establishing comprehensive legal and operational frameworks, 488–490
    stakeholder responsibilities and liability distribution, 483–484
Cyber resilience, 263
Cybersecurity, 1, 400–401
  challenges in, 11–12
  convergence of, 3–4
  emerging opportunities, 13–14
  evolution of, 4–5
  frameworks, 7–9, 8*f*
  in modern digital ecosystems, 1–2
  social solutions for, 449–450
  threats, 338
Cyber threats, 5

D

Data analysis, 413–417
  distribution of network protocols *versus* attack category, 415–416
  distribution of services, 414
  distribution of service type *versus* attack category, 414–415
  distribution of target variable, 413
  feature importance, 416–417
  and feature influence, 408
Data authentication, 370
Databases (DBs), 136*f*, 139*f*
Data breaches, 433–434
Data collection, 69–71
Data confidentiality, 370
Data-driven decision-making, 275
Data-driven operations, 290
Data Encryption Standard (DES), 4–5
Data exfiltration, 275
Data flow complexity, 485
Data integrity, 181, 366, 370
Data leakage, 370
Data management, 491
Data manipulation, 178, 294
Data marketplaces, 181
Data poisoning, 294

Data preprocessing, 72, 408
  encoding categorical variables, 72
  identification of categorical columns and normalization, 72
  splitting data, 72
Data privacy, 370–372
Data Protection Act (Kenya), 476–479
Data Protection Act 2018 (UK), 475
Data regulations, 269–270
Data retention and deletion, 480
Data security, 370–372
Data storage systems, 361
Data tampering, 370
Data use agreement (DUA), 255
Debian Linux repository, 226
Decentralization, 367
Decentralized applications (DApps), 179
Decentralized approach, 372
Decentralized architectures, 9–10, 356, 431–432
Decentralized autonomous organizations (DAOs), 181
Decentralized computing, 9–10
Decentralized security decision-making, 33–38
  implementation strategies, 35–36
    coordination mechanisms, 36
    distributed consensus protocols, 35
    dynamic trust evaluation algorithm, 36
    local decision-making algorithms, 35–36
  performance considerations, 36–38
    latency impact analysis, 36–37
    resource utilization, 38
    scalability analysis, 38
  theoretical framework, 33–35
    decision theory application, 34
    risk assessment models, 34
    trust evaluation mechanisms, 34–35
Decentralized security mechanisms, 435–436
Decentralized training, 263
Decisional Diffie-Hellman assumption, 184
Decision-making processes, 433
Decision theory application, 34
Decision trees (DT), 109
Decompilation techniques, 226
Deep learning (DL), 65–68, 96, 322–323
Deep reinforcement learning, 97–98, 399
Defense in depth principle, 31, 31*f*
Defensive distillation, 15
Defensive walls against sophisticated ML-orchestrated attacks (DWASMA), 277, 289–290, 305–307
  adaptive response mechanism, 297–298
  challenges in, 295–296
  characteristics of, 293–295
    emerging threat dimensions, 294–295
    proactive defense strategies, 295
  components of, 296
  data-driven operations, 290
  dynamic threat landscape, 289
  evaluating the effectiveness of, 299–300
  future directions and emerging trends in defense strategies, 309
  incorporating human expertise in defense, 298
  key components of, 289
  key machine learning attack strategies, 290–293
    adversarial machine learning attacks, 290
    autonomous vehicle vulnerabilities, 292
    credential stuffing and account takeover attacks, 290–291
    healthcare fraud and abuse detection, 293
    ML-driven financial fraud, 292
    ML-driven social media manipulation, 291
    ML-enhanced supply chain attacks, 292–293
    ML-powered insider threat detection, 292
    ML-powered malware obfuscation, 291–292
    ML-powered phishing campaigns, 291
    voice and audio deepfakes, 291
  key risks, 290
  notable tactics, 289–290
  proposed defensive walls against sophisticated ML-orchestrated attacks, 300–305, 305*b*
    ML-driven attack detection strategy, 303–304
    network flow and load balancing in edge computing, 304
    public and private key security model, 304
    quantum-resistant encryption model, 305
  role of machine learning in defensive strategies, 296–297
  sophisticated adversaries, 289
  threat detection and anomaly identification, 297
Delegated proof of stake (DPoS), 179, 380
Denial of service (DoS) attacks, 30, 105, 373, 399
Destination Packets (dpkts), 407
DevOps pipeline, 100
Dialogs.dll, 352–355
DIDS. *See* Distributed intrusion detection systems (DIDS)
Differential privacy (DP), 123–124, 128–129, 246–247
Digital signatures, 367, 370
Digital transformation, 377
Digital twins (DT), 96–97
Discrete logarithm problem, 184
Discretionary access control (DAC), 382
Distributed consensus protocols, 35
Distributed defense mechanisms, 15
Distributed denial-of-service (DDoS) attacks, 105, 344–345, 434
Distributed intrusion detection systems (DIDS), 3, 17–18

Distributed ledger, 367
Distributing tasks, 373
Docker, 85, 88
Domain, 300
Domain A, 301*f*
Domain Name System (DNS), 407
Doomslug consensus mechanism, 192–193
DoS attacks. *See* Denial of service (DoS) attacks
DP. *See* Differential privacy (DP)
Drone-mounted base station, 163
DWASMA. *See* Defensive walls against sophisticated ML-orchestrated attacks (DWASMA)
Dynamic access control policies, 378
Dynamic allocation, 98
Dynamic and context-aware behavior, 294
Dynamic microservice scheduling algorithm, 94–95
Dynamic resource allocation, 384–385
Dynamic risk assessment, 375
Dynamic threat landscape, 289
Dynamic trust evaluation algorithm, 36, 37*f*

E

Ebdxobys.exe, 351, 352*t*, 353*f*, 354*f*, 355–356
EC. *See* Edge computing (EC)
EC-inspired IoT (EC-IoT), 65–68
Edge AI, 4, 7
Edge computing (EC), 1, 63–64, 85, 87, 155, 261–262, 362–363, 382–383, 395–396, 431–432
  adversarial defenses in, 14–15
  algorithmic fairness and bias, 441
  applications of, 362–363
  architecture, 363*f*
  assisted free space optical wireless communications, 162–164
  assisted optical fiber-wireless communications, 161*f*, 164–165
  assisted optical wireless communications and positioning, 156–162
    indoor OWC, 157, 160*t*
    optical wireless positioning, 160–162
    outdoor OWC, 158–160, 160*t*
  balancing decentralization and centralized oversight, 459
  balancing innovation and regulation, 508
  case studies on accountability in edge computing incidents, 486–488
    industrial Internet of Things edge computing failure, 487–488
    smart city traffic management system breach, 486–487
  challenges in regulatory compliance for, 479–481, 481*f*
    accountability and transparency, 480
    consent management, 479
    data localization and cross-border transfers, 479
    data retention and deletion, 480
    implementation of data subject rights, 480
    security measures, 480–481
  clear accountability and liability distribution, 507
  community-based security models, 439–440
  complex liability challenges in, 484–486
    data flow complexity, 485
    evidence collection and preservation, 485
    insurance and risk transfer issues, 486
    jurisdictional complexities, 485
    shared resource implications, 486
    stakeholder interdependency issues, 484
    standard of care determination, 485
    technical complexity challenges, 484
    technology evolution impact, 485
    temporal attribution challenges, 485
  continuous adaptation to evolving threats, 459
  convergence of, 3–4
  cross-border data governance, 507
  cybersecurity defensive walls in, 161*f*
  definition, 362
  development of, 6–7
  in distributed architectures, 2–3
  dynamic microservice scheduling mechanism for, 94–95
  education and training, 508
  emerging opportunities, 13–14
  emerging regulatory frameworks and policy initiatives, 490–502
    current and proposed regulatory frameworks specific to cyber edge computing, 490–492
    impact of frameworks on development and adoption, 493–499
    role of policymakers and industry stakeholders in shaping the regulatory landscape, 499–502
  emerging regulatory trends specific to edge computing and cybersecurity, 502–503
    artificial intelligence-driven compliance monitoring, 502–503
    cross-border data governance, 503
    edge-specific privacy requirements, 503
    zero trust architecture requirements, 502
  emerging strategies for regulatory compliance in, 481–483, 482*f*
  environment, 376*t*
  establishing comprehensive legal and operational frameworks, 488–490
    compliance and regulatory alignment, 488
    cost allocation and budget planning, 489
    dispute resolution mechanisms, 489
    documentation and communication requirements, 489

future-proofing measures, 490
incident response and resolution protocols, 488
insurance and risk management, 489
performance monitoring and evaluation, 489
stakeholder responsibility delineation, 488
technical accountability measures, 488
technology evolution considerations, 489
third-party management, 489
ethical and social solutions for cybersecurity in, 444–451
ethical framework development, 448–449
evaluation metrics, 451
integration of ethical design, 450–451
social solutions for cybersecurity, 449–450
ethical compliance as strategic priority, 459
ethical concerns in computing, 439
ethical frameworks for cybersecurity in, 435–436
features and benefits of, 362
future-proofing regulatory frameworks, 508
healthcare systems, 383
holistic approach to ethical and social integration, 460
implementing social and ethical solutions in edge computing cybersecurity, 452–457
challenges in implementation, 456–457
enhanced cybersecurity resilience, 452–453
ethical compliance, 454–456
increased user trust, 453–454
importance of cybersecurity in, 432–433
importance of privacy-preserving technologies, 507
intrusion detection in distributed edge systems, 17–18
IoT networks, 383
limitations and future research directions, 165–168
limitations of social and ethical solutions to combat threats in, 461
machine learning at the edge, 15–16
need for adaptive regulatory frameworks, 506
overview of, 432
power of community-driven models, 458
predictions for future legal and policy developments, 503–504
environmental impact considerations, 504
quantum-ready requirements, 504
resource-aware regulation, 504
unified global standards, 503
principles, 8*f*, 9–10
proactive security measures, 507
recommendations for further research and policy development, 504–506
future research directions, 506
implementation guidelines, 505
policy development recommendations, 505
technical research priorities, 504–505
regulatory frameworks, 441–442
research motivation and problem statement, 436–437
security challenges in, 368–379
adaptive security architectures, 374–375
data security and privacy concerns, 370–372
holistic security approaches, 377–379
threats and vulnerabilities, 373–374
virtualization-specific challenges, 375–377
smart cities, 383
social and ethical implications of cyber attacks, 433
social concerns in, 442–444
social solutions to cybersecurity challenges, 435
stakeholder collaboration, 508
stakeholder responsibilities and liability distribution, 483–484
technological and ethical innovations to strengthen cybersecurity, 436
transparency as trust-building mechanism, 459
understanding cyber attacks, 433–435
case studies of notable attacks, 434–435
common cyber threats in, 433–434
impact of cyber attacks on society and ethic, 434
Edge computing authentication techniques, 328–331
biometric-based access control mechanism, 329
evaluating metrics, 329–330
traditional access control mechanism, 328–329
password-based access control, 328
smart card-based access control, 329
token-based access control, 328–329
Edge computing security, 21
architectural security foundations, 28–33
architectural design principles, 30–32
core security requirements, 29–30
reference architecture, 32–33
context and motivation, 21–22
current security challenges, 26
resource optimization, 26
trust management, 26
decentralized security decision-making, 33–38
emerging solutions, 27
AI-enhanced security, 27
blockchain integration, 27
emerging technologies, 56–57
artificial intelligence/machine learning integration, 56
novel architectural patterns, 57
quantum-safe security, 56–57
evolution of edge security architecture, 25–26
experimental setup, 50–52
configuration parameters, 50
performance measurement, 51–52
results, 52
future impact of, 59–60

healthcare edge computing, 44–45
industrial IoT security, 41–43
key contributions, 24–25
key research contributions in, 28*t*
limitations and constraints, 55
long-term evolution of, 58
microservice security architecture, 38–41
practical implications, 55–56, 59
research challenges, 22
research gaps, 27–28
research objectives, 23–24
research opportunities, 57
simulation methodology, 45–50
network model, 45–46
security event generation, 46–50
smart city infrastructure, 43–44
theoretical contributions, 58–59
Edge devices, 264–265
Edge servers, 97–98, 331
Edge-specific encryption protocols, 377–378
Education, 508
Edwards-curve Digital Signature Algorithm (EdDSA), 195
Elliptic curve cryptography (ECC), 276–277
encrypts communication, 306–307, 310*f*
Employee training, 374
Encrypted information, 300
Encryption function, 302
Endpoint protection systems, 344–345, 375
Energy consumption, 98
Energy-efficient blockchain technologies, 388
Epochs, 189
Equal access, 261
Ethereum, 179, 188, 385
Ethical-by-design protocols, 450–451, 454, 455*t*
Ethical hacking, 435
European Union (EU), 475, 499
Evaluating metrics, 329–330
Evaluation index, 235*t*
Evaluation metrics, 451
Evasion techniques, 294
Event stream processing (ESP), 65–68
Explainable AI (XAI), 308

F

F1 score, 111
Facial recognition, 318, 324, 326*t*
Fairness, 255
False positive rate (FPR), 145
Fast Gradient Sign Method (FGSM), 69–72, 73*f*, 82
Fast Reed-Solomon Interactive Oracle Proof (FRI), 199
Federated averaging (FedAvg), 250
Federated blockchain, 368
Federated learning (FL), 2, 65–68, 129–130, 147, 246, 248*f*
challenges in, 12*f*
communication efficiency of, 251–252, 252*t*
ethical and regulatory considerations in, 254–255
privacy preservation in, 252–254
properties of, 249–251
FedProx, 255
Fiber-wireless (FiWi) communications, 164–165
5G networks, 3, 6
Fifth-generation (5G) network, 63–64
File Transfer Protocol (FTP), 65–68, 407
Final block proof, 203–204
Finance, 325
Fingerprint scanning, 318, 324, 326*t*
Firmalice, 224–225
FL. *See* Federated learning (FL)
FL-RAEC, 66*t*
Fog computing, 96–97
Fork choice rule, 192
Fuzzy extractor-based scheme, 322–323
Fuzzy logic, 98

G

GANs. *See* Generative adversarial networks (GANs)
Garbled circuits, 258–259, 268
Gas model, 189
Gaussian copula model, 131
based on differentially private data, 131–132
Gaussian distribution, 131–132
Gaussian functions, 165–168
Gaussian noise, 252–253
General Data Protection Regulation (GDPR), 13, 245–246, 254–255, 435–436, 455, 473, 475
Generative adversarial networks (GANs), 144–145, 319–321, 402
Genesis block, 198, 365
Genetic algorithms (GA), 107–108
GENI testbed, 319–321
Geometric median method, 254
Ghidra plugin, 234
Gini index, 108
GitHub, 69–72
Global data protection laws, 473–479
California Consumer Privacy Act and California Privacy Rights Act (United States), 473
Data Protection Act (Kenya), 476–479
General Data Protection Regulation (EU), 473
Lei Geral de Proteção de Dados (Brazil), 474
Nigeria Data Protection Regulation, 476
Personal Data Protection Act (Singapore), 474–475

Personal Information Protection and Electronic Documents Act (Canada), 474
Privacy Act 1988 (Australia), 475–476
Protection of Personal Information Act (South Africa), 476
UK General Data Protection Regulation and Data Protection Act 2018 (UK), 475
Google, 127, 360–361
Google BeyondCorp, 99–100
Google Cloud Engine, 89
Gradient masking, 14–15
Gradient Sign Method Adversary (GSMA), 77–78, 80, 82
Graph attention network (GAN), 66*t*
Graphics processing unit (GPU), 157–158
Greedy algorithm, 162–163
GridSearch, 73–74
Grid Search Mean Test Scores, 76–77
GSMA. *See* Gradient Sign Method Adversary (GSMA)

H
Hardcoded login credentials, 222
advantages, 240
experiment, 233–239
implementation, 234
measure of accuracy, 234–235
socket search, 238–239
string search, 236–238
whole search, 235–236, 236*t*
future research directions, 241
limitations, 240
overview, 228
in Q-See DVR, 224*f*
security implications, 240
socket search, 230–233
string search, 229–230
summary of results, 239–240
Hash, 366
Healthcare, 123, 245–246, 325, 362, 432
Healthcare edge computing, 44–45
compliance aspects, 44
performance metrics, 45
privacy considerations, 44
security implementation, 44
Healthcare fraud, 293
Healthcare systems, 383
Health Insurance Portability and Accountability Act (HIPAA), 13, 491
Heatmap, 76, 76*f*
HermScan, 227
Heuristic algorithms, 97–98
Hierarchical filtering and progressive detection model (HFPD-IDS), 108
Hill-climbing attacks, 322–323
Histogram of oriented gradients (HOG), 400
Holistic security approaches, 377–379
Homomorphic encryption (HE), 247, 257–258
Host-based intrusion detection systems (HIDS), 9, 108
Host-based microsegmentation, 89
Human activity recognition system, 128
Human expertise, 298
Human input, 298
HumIDIFy, 225
Hybrid blockchain, 368
Hybrid IDS, 108
Hyperbolic tangent kernel, 411–412
Hyperledger Fabric, 384
Hypertext Transfer Protocol (HTTP), 65–68, 407
Hypertext Transfer Protocol secure (HTTPS), 65–68
Hypervisor-centric microsegmentation, 102

I
Identity and access management (IAM), 99
Identity-based access control (IBAC), 324
Identity management, 360–361
Identity-Specific Encrypt-Decrypt architecture, 127–128
IDS. *See* Intrusion detection systems (IDS)
IDUE_OUE methods, 134
IDUE_RAPPOR methods, 134
IIoT security. *See* Industrial Internet of Things (IIoT) security
Immutability, 178, 367
Incident response, 41
Indicators of compromise (IOCs), 352
Indoor OWC, 157, 160*t*
Industrial automation, 325
Industrial Internet of Things (IIoT) security, 4, 41–43, 123, 362, 402
architecture implementation, 42
edge computing failure, 487–488
performance analysis, 42–43
scenario description, 42
Industry stakeholders, 499–500
Ineffective identification, 370
Informed consent, 255
Infrastructure as a service (IaaS), 360
Institute of Electrical and Electronics Engineers (IEEE), 490
Integrated security framework, 377
Intelligent zero-trust architecture (i-ZTA), 99
Interactive ZKPs, 184
International Mobile Equipment Identity (IMEI), 72
International Organization for Standardization (ISO), 490
Internet Control Message Protocol, 407

Internet of Things (IoT), 1–2, 63–64, 96, 173, 178–182, 221, 319–321, 360, 432
networks, 383
opportunities and challenges, 180*f*, 181–182
Internet-of-Vehicles, 319–321
Interoperability, 181, 186
Intrusion detection systems (IDS), 2–3, 9, 105, 339, 375, 400
datasets description, 109–110
in distributed edge systems, 17–18
experimental results, 111–117
algorithm, 113
binary classification, 112–113
MQTTset dataset, 117
multiclass classification, 114
UNSW-NB15 dataset, 112
feature reduction, 111
IoT. *See* Internet of Things (IoT)
Iris scanning, 326*t*

J
Jacobian-based Saliency Map Attack (JSMA), 69–72
Java SE Development Kit 11 (JDK 11), 234
Jurisdictional complexities, 485

K
Kaggle, 69–72
k-anonymity, 144
Kanto region, 141
KDDCup99 dataset, 108
Know Your Customer (KYC) processes, 184
Krum algorithm, 253–254
Kubernetes, 85, 88–89, 384

L
Lambert W function, 133
Large language models (LLMs), 125–126, 131*f*, 143, 227, 241
limitation of, 148–149
and privacy, 148
Latency impact analysis, 36–37
Latency reduction, and a load-balancing algorithm (LRLBAS), 97
Lei Geral de Proteção de Dados (LGPD), Brazil, 474
Light emitting diode (LED) technology, 160
Light fidelity (LiFi), 157
Linear support vector machine, 409–410, 417, 420, 422*f*
Linux, 330
LLMs. *See* Large language models (LLMs)
Local decision-making algorithms, 35–36
Local dynamic map (LDM), 158–159
Location Area Code (LAC), 72
Logistic regression (LR), 109

M
Machine learning (ML), 3, 63–64, 165, 245–246, 275, 346, 350, 360–361, 395, 439
in defensive strategies, 296–297
federated learning, 246
secure distributed machine learning, 247
secure multiparty computation, 247
Macro average, 413, 425
Malicious adversaries, 258
Malware and ransomware infections, 434
Mandatory access control (MAC), 382
Man-in-the-middle attacks, 105, 373, 399, 434
Market1501 dataset, 127–128
Medical image analysis and processing, 325
Merkle proofs, 186
Merkle tree, 366
Metrics, for privacy and data security., 371*t*
Micropayments, 181
Microsegmentation, 89–90, 90*f*, 91*f*, 378
lack of host-level visibility, 102–103
lack of support for container workloads, 102
scalability cost, 101
static policies, 102
Microservice architecture (MSA), 94–95
Microservices, 86–89
architecture, 88*f*
containerization of, 96–99
and containers, 87–89
in edge computing, 94–96
microsegmentation, 89–90, 99–101
Microservice security architecture, 38–41
deployment considerations, 40–41
configuration management, 41
incident response, 41
security monitoring, 41
design patterns, 39–40
API security, 39
container security, 40
service mesh security, 39
security controls, 40
access control mechanisms, 40
secret management, 40
service-to-service authentication, 40
Microsoft, 360–361
Microsoft Azure, 89
Microsoft Azure Zero Trust architecture, 99–100
Mina protocol, 188
Mirai botnet attack, 434–435
ML. *See* Machine learning (ML)
ML-driven attack detection strategy, 303–304
ML-driven financial fraud, 292
ML-driven social media manipulation, 291
ML-enhanced supply chain attacks, 292–293

ML-powered insider threat detection, 292
ML-powered malware obfuscation, 291–292
ML-powered phishing campaigns, 291
Mobile edge computing (MEC) platform, 362
MQTTset dataset, 107, 110*t*, 117
Multi-authority attribute-based encryption scheme, 319–321
Multifactor authentication, 378
Multiparty computation (MPC), 129–130
Mutual TLS (mTLS), 40

N
Naive Bayes (NB), 109
National Institute of Standards and Technology (NIST), 490
National Security Agency, 231
NEAR. *See* Network of Efficient, Agile, Reliable blockchains (NEAR)
Network-based intrusion detection systems (NIDS), 9, 108
Network-based microsegmentation, 101
Networking, 331
Network-layer defense mechanisms, 349
Network model, 45–46
Network of Efficient, Agile, Reliable blockchains (NEAR), 174, 176, 188–193, 218–219
  architecture overview of, 189–190
  block structure, 197*f*
  Doomslug consensus mechanism, 192–193
  linked proofs, 198*f*
  proving block entities, 197*f*
  sharding and Nightshade, 190–192
  signature verification, 196*f*
  and specific blockchain architectures, 176
  zero-knowledge proofs for block finality in, 193–204
    detailed analysis of system components, 199–203
    overview of, 196–199
    Plonky2, 199
    proof aggregation and final block proof, 203–204, 203*f*
    system limitations and constraints, 204
    system overview and design principles, 194–196
Network security threats, 373
Neural network (NN) algorithms, 400
Newton-Raphson method, 133
Next_bp_hash, 197, 202–203
Next-generation firewalls (NGFWs), 339
Nigeria Data Protection Regulation (NDPR), 476
Nightshade model, 189–192
Nightshade sharding mechanism, 191
  chunk-only producers, 191
  cross-shard transactions, 191
  dynamic sharding, 191
  fraud proofs and data availability, 191
  hidden sharding, 191
  state sharding, 191
Noninteractive zero-knowledge proofs (NIZKs), 184
Nonlinear function, 322–323
Novel architectural patterns, 57

O
Oblivious transfer (OT), 247, 258
OneHotEncoder encoding technique, 72
OpenCV, 331
Open Neural Network Exchange (ONNX), 16
OpenStack, 165
Open Worldwide Application Security Project (OWASP), 222
Operating system, 330
Optical wireless communication (OWC), 155
  indoor OWC, 157
  outdoor OWC, 158–160
Optical wireless positioning (OWP), 155–156, 160–162
Optimization modeling, 97–98
OptMean methods, 134–135
OptMode methods, 134–135, 137
Orchestration, 375
Outdoor OWC, 158–160, 160*t*

P
Parent function, 233
Particle swarm optimization, 97
Password-based access control, 328
PCA. *See* Principal component analysis (PCA)
Performance analysis, 42–43, 174
Performance metrics, 45, 78–81, 94–95, 205–206
  for block hash verification with real NEAR blocks, 208*t*
  for block hash verification with synthetic data, 207*t*
  classification report, 78
  comparison of numeric results based on existing works, 81
  confusion matrix, 79, 79*f*
  for prove_bp_hash function, 213*t*
  for prove_current_block function, 215*t*
  for prove_header_hash function, 215*t*
  for prove_valid_keys_stakes_in_validators_list function, 211*t*
  receiver operating characteristic curve analysis, 80
  for signature verification with real NEAR blocks, 209*t*
Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge (PLONK), 199
Personal Data Protection Act (PDPA), Singapore, 474–475
Personal Information Protection and Electronic Documents Act (PIPEDA), Canada, 474

Personalization, 293
Personally identifiable information (PII), 124
Physical layer security (PLS) technology, 162–163
Physical security thefts, 373
Platform as a service (PaaS), 360
Plonky2 framework, 195, 199
Poisson distribution, 132–133
Policy-based access control (PBAC), 324
Policymakers, 499
Polymorphism, 294, 341
Polynomial support vector machine, 411, 423
Practical Byzantine fault tolerance (PBFT), 179, 380
Precision, 75, 412
PreGAN, 66*t*
Principal component analysis (PCA), 107, 107*f*, 111
printHardCoded function, 230, 230*b*, 233
printIncomingCalls function, 233, 233*b*
printOutgoingCalls function, 233, 233*b*
printReference function, 233, 233*b*
Privacy, 252–253
  leaks, 370
  preservation, 263
Privacy Act 1988 (Australia), 475–476
Privacy-aware access control, 322–323
Privacy-preserving techniques, 24, 255
Privacy-preserving transactions, 184
Private blockchain, 368
Proactive security measures, 507
Probability distribution function (PDF), 131
Proof aggregation, 203–204, 203*f*
Proof of authority (PoA), 380
Proof of burn (PoB), 380
Proof of stake (PoS), 179, 367, 380
Proof of work (PoW), 179, 367, 380
Protection of Personal Information Act (POPIA), 476
Public and private key security model, 304
Public blockchain, 367
Public-private partnerships, 435
Python library, 75
PyTorch Mobile, 7, 16

Q

Q-See DVR, 224*f*
  hardcoded login password in, 237*f*
  string search successfully found new login password in, 237*f*
Quality control, 325
Quality of service (QoS), 94–95
Quantization techniques, 16
Quantum computing, 14
Quantum-resistant encryption model, 305
Quantum-safe security, 56–57

R

Radial basis function (RBF), 396
Radial basis function support vector machine, 410, 422, 423*f*
radient Sign Method Adversary (GSMA), 77
Radio Access Type (RAT), 72
Radio frequency (RF), 155
Random forest (RF), 400
Random forest classifier algorithm, 73–74, 74*t*, 113*b*
Random forest classifier model training, 75*t*
Raspberry Pi 4 devices, 96
RaySharp DVR, 237
Real block analysis, 206
Real smart house experiment, 137–141
Real-time processing, 10
Recall, 75, 111, 412–413
Receiver operating characteristic (ROC) curve, 75, 80, 80*f*
REcompile, 226
Reference architecture, 32–33
  component interaction patterns, 32–33
  layered security model, 32, 32*f*
  security boundaries, 33, 33*f*
Regulatory frameworks, 441–442
Reidentification
  blockchain-based method for sensitive data, 129
  bloom filter and reidentification, 145
  considerations on advanced DP techniques, 144–145
  differential privacy, 128–129
  estimating occurrence probability, 132–133
  estimating risk of, 127–128
  evaluation, 134–144
    experiments on computation time, 141–143
    real smart house experiment, 137–141
    results on differentially private datasets, 137
    results on nonprivatized datasets, 135–137
    utilizing large language models, 143–144
  future directions for enhancing differential privacy, 146–147
  Gaussian copula model based on differentially private data, 131–132
  implications of reidentification risks in real-world scenarios, 146
  large language models and privacy, 148
  limitations of current privacy techniques, 147–148
  secure computation of sensitive data, 129–130
  using existence in each table, 133–134
Remote Access Trojans (RATs) attacks, 337, 340
  connection, 344
  data theft and manipulation, 345
  infiltration, 342–343
  installation, 343–344
  methodology, 351–355
  remote control and monitoring, 344–345

Representation state transfer (REST), 95
Resource constraints, 181
Resource optimization, 26, 98
Resource utilization, 38
Retail, 362
Reverse engineering framework, 226
Risk assessment models, 34
Rivest–Shamir–Adleman (RSA) algorithm, 5
Roadside units (RSUs), 159–160
Robotics control, 325
Robust aggregation methods, 246–247
Robust authentication protocols, 374
Robust cybersecurity, 432–433
Robust defenses, 14
Robust identification, 370
ROC curve. *See* Receiver operating characteristic (ROC) curve
Role-based access control (RBAC) methods, 324, 378, 382

S

Salesforce, 360–361
Scalability, 181, 194, 293, 375
Scalability analysis, 38
Scalable transparent arguments of knowledge (STARKs), 184
Scikit-learn, 75
SDML. *See* Secure distributed machine learning (SDML)
Secret management, 40
Secret sharing (SS), 247, 257–258
Secure aggregation, 252–253, 269
Secure distributed machine learning (SDML), 246–247, 248*f*, 261–267
  architecture, 264–267
    aggregation servers, 265
    communication protocols, 266–267
    cryptographic protocols, 265–266
    edge devices, 264–265
  motivation behind secure distributed machine learning, 262–263
Secure information and event management (SIEM), 375
Secure multiparty computation (SMPC), 246–247, 248*f*
  advanced cryptographic techniques for, 258–260
  ethical and regulatory considerations in, 260–261
  high-level architecture of, 257*f*
  security methods of, 256–258
SecureReID, 127–128
Secure Sockets Layer, 414–415
Secure virtualization practices, 377
Security automation, 378
Security awareness training, 378
Security event generation, 46–50
Security measures, 480–481
Security monitoring, 41
Self-driving vehicles, 399
Self-executing agreements, 179
Self-governance, 370
Semantic flow graph, 226
Semihonest adversaries, 258
Semisupervised learning, 297
Sending out information, 300
Service mesh security, 39
Service-oriented architecture (SOA), 95
Service-to-service authentication, 40
SHA-256, 194
SHapley Additive exPlanations (SHAP), 109
Sharding algorithm, 189–192
Sigmoid support vector machine, 411–412, 422, 424*f*
Signature-based methods, 350
Signatures, 200–201
Simple Mail Transfer Protocol (SMTP), 65–68
Simplified payment verification (SPV), 173–174
6G networks, 14, 155
Smart card-based access control, 329
Smart cities, 123, 325, 362, 383, 432
Smart city infrastructure, 43–44
  architectural solution, 43–44
  results and analysis, 44
  security requirements, 43
Smart city traffic management system breach, 486–487
Smart contracts, 27, 179, 190, 365, 372, 384
Smart Detection Tools, 296
Smart homes, 325
SOA. *See* Service-oriented architecture (SOA)
Social engineering, 340
Socket search method, 225, 228, 230–233, 231*f*, 232*b*, 232*f*, 238–239
Software as a service (SaaS), 360
Software-defined networking (SDN), 108
Software vulnerabilities, 373
SolarWinds supply chain attack, 434–435
Source Packets (spkts), 407
Speeded-Up Robust Features (SURF), 400
Stakeholders, 339, 457
  collaboration, 508
  interdependency issues, 484
  responsibilities and liability distribution, 483–484
    cloud service provider accountability, 484
    device manufacturers' role and obligations, 483
    network service providers' responsibilities, 483–484
State transition function, 191
Static analysis, 226, 349
Stolen data, 337–338
StraightTaint, 225–226

Strcmp() function, 225
Stringer, 225
String search method, 222, 225, 228–230, 229*f*, 230*b*, 236–238, 236*t*
Strncmp() function, 222
Structured Query Language, 414–415
Succinct noninteractive arguments of knowledge (SNARKs), 184
Supervised learning, 297
Supply chain, 325
Support vector machines (SVMs), 395, 398*f*
  addressing research gaps, 402–403
  applications of, 401
  classification report, 420–423
  comparison of evaluation scores of all models, 423–425
  confusion matrices, 417–419, 419*f*
  in cybersecurity, 400–401
  data analysis, 413–417
    distribution of network protocols *versus* attack category, 415–416
    distribution of services, 414
    distribution of service type *versus* attack category, 414–415
    distribution of target variable, 413
    feature importance, 416–417
    and feature influence, 408
  data preprocessing, 408
  dataset source and relevance, 406
  dataset structure and attributes, 406–408
  evolution of edge computing and associated issues, 399
  model building, 408–413
    linear support vector machine, 409–410
    macro average, 413
    polynomial support vector machine, 411
    precision, 412
    radial basis function support vector machine, 410
    recall, 412–413
    sigmoid support vector machine, 411–412
    weighted average, 413
  vulnerability management in edge networks, 401–402
Synthetic data analysis, 206
System.dll, 354–355

T

Target data breach, 434–435
TCP32764 router's program, 237
Tenda router, 238
Tendermint, 380
TensorFlow Lite, 7, 15–16
Third-party management, 489
Threat detection and anomaly identification, 297
Threat intelligence integration, 375
Threats, 373–374
Threshold cryptography, 258
Time of execution, 329
Token-based access control, 328–329
Traceability, 181
Traditional access control mechanisms, 319–321
Traffic analysis, 349
Training, 508
Transmission control protocol (TCP), 230, 407
Transparency, 178, 255, 261, 367, 480
  as trust-building mechanism, 459
Transport layer security (TLS), 39, 266
Trusted platform modules (TPMs), 340
Trust evaluation mechanisms, 34–35
Trust management, 26
TurboPLONK, 199

U

Ultrareliable and low latency communication (URLLC), 159–160
Uniform resource locators (URLs), 69–72
Unmanned aerial vehicles (UAVs), 65–68, 155–156, 162
Unsupervised learning, 297
UNSW-NB15 dataset, 106*t*, 107, 111–112
User-centric approach, 457, 461
User datagram protocol (UDP), 230, 407
Utility computing, 360–361

V

ValidatorList, 202–203
Validators, 189
Value-driven Ownership of Data and Accessibility Network (VODAN), 245–246, 251–252, 262, 268
Vendor risk management, 379
Virtualization technology, 360–361
Virtualized environments, 379
Virtual machines, 361
Virtual reality (VR), 157–158
Visible light communications (VLC), 157
Visualizations, 76–77
VODAN. *See* Value-driven Ownership of Data and Accessibility Network (VODAN)
Voice and audio deepfakes, 291
Voice recognition, 318, 324, 326*t*
Voting systems, 186
Vulnerabilities, 373–374
Vulnerability assessments, 341

W

Weighted average, 413, 425
Welcome.html, 354–355

Whole search, 235–236, 236*t*, 239
Windows, 330
Windows API functions, 349
Windows Error Reporting (WER), 355
Windows Native API system service calls, 349

X

x86 server, 165
XGBoost classifier algorithm, 111–112, 114*b*

Z

Zero-day exploitation, 294
Zero-knowledge proofs (ZKPs), 13, 27, 174, 258
  applications in blockchain, 184–186, 185*f*
  blockchain scalability and sharding, 175
  in blockchain systems, 176
  block finality verification using, 195*b*
  block hash verification performance, 207–208
    next block producer hash verification performance, 213–214
    proof aggregation and final block verification performance, 215–216
    real block analysis, 207–208
    signature verification performance, 209–211
    synthetic data analysis, 207
    validator key and stake verification performance, 211–213
  contributions of, 174
  fundamentals of, 182–184
  light clients and resource-constrained environments, 176
  methodology and implementation details, 205–206
    cryptographic primitives, 205
    implementation specifics, 205
    performance metrics, 205–206
    testing environment, 205
  NEAR Protocol, 188–193
    architecture overview of, 189–190
    Doomslug consensus mechanism, 192–193
    sharding and Nightshade, 190–192
    and specific blockchain architectures, 176
  organization of, 174–175
  research gaps and our contribution, 176–178
  as solution for light client scalability, 186–188, 187*f*
  types of, 183*f*
Zero-trust architectures (ZTAs), 7, 9, 100, 339
Zero-trust environments, 247
Zero trust models, 435–436
Zero-trust security models, 86, 377
ZKPs. *See* Zero-knowledge proofs (ZKPs)