Navigating Cybersecurity and Privacy in the Evolution of Smart Urban Ecosystems

Asmaa Mahfoud Alhakimi
https://orcid.org/0000-0002-4038-5203
Management and Science University, Malaysia

Safaa Najah Saud Al-Humairi
https://orcid.org/0000-0001-5978-7651
Management and Science University, Malaysia

Saddaf Rubab
https://orcid.org/0000-0003-3208-5275
University of Sharjah, UAE

I. Wayan Budi Sentana
https://orcid.org/0000-0003-3559-5123
Bali State Polytechnic, Indonesia

IGI Global
Scientific Publishing
Publishing Tomorrow's Research Today

Table of Contents

Preface xvi

Acknowledgment xxii

Introduction xxiii

Chapter 1
An Overview of Smart Cities Covering Applications, Challenges, and Emerging Trends 1
Ravesa Akhter, National Institute of Technology Srinagar, India
Rabiya Akhter, University of Kashmir, India
Insha Shafi, National Institute of Technology Srinagar, India
Shabir Sofi, National Institute of Technology Srinagar, India

Chapter 2
When Nature Meets Code: Governing Grey Data for Cybersecurity and Sustainability in Smart Cities 35
Ahgalya Subbiah, Management and Science University, Malaysia

Chapter 3
Blockchain Beyond Cryptocurrency: A Decentralized Approach to Urban Security 63
Yahaya Saidu, Universiti Teknologi PETRONAS, Malaysia & Taraba State University, Jalingo, Nigeria
Shuaibu Yau, Federal University Birnin Kebbi, Nigeria
Daniel Tonye Oyefidein, Universiti Teknologi PETRONAS, Malaysia
Aliyu Garba, Universiti Teknologi PETRONAS, Malaysia
Dahiru Adamu Aliyu, Universiti Teknologi PETRONAS, Malaysia

Chapter 4
Cyberattacks: Blockchain Beyond Cryptocurrency - A Decentralized Approach to Urban Security 99
Syed Hassan Imam Gardezi, Union Investments LLC, UAE
Swaroop Mohanty, ACCFK, Amity University, Kolkata, India
V. Bharathi, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India
T. C. Manjunath, Rajarajeswari College of Engineering, India
Syed Muqthadar Ali, CVR College of Engineering, India
F. Shabina Fred Rishma, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, India
P. Selvakumar, Department of Science and Humanities, Nehru Institute of Technology, Coimbatore, India

Chapter 5
Cybersecurity at the Edge: Defending Decentralized Cities in a Borderless Threat Landscape 127
Fadi Bata, Applied Science Private University, Jordan
Mohammad Albadareen, Hashemite University, Jordan
Bashar Khassawneh, Amman Arab University, Jordan
Mahmoud Aljawarneh, Applied Science Private University, Jordan
Qais Al-Na'amneh, Applied Science Private University, Jordan
Ayoub Alsarhan, Hashemite University, Jordan
Ahmad Saleh Alhazaimeh, King Abdaulaziz University, Saudi Arabia

Chapter 6
Enhancing Cybersecurity, Privacy Innovation, and E-Government Readiness in Smart Cities: A Framework for Awareness and Resilience 159
Mohammed Hussain Alsaad, Management and Science University, Malaysia
Muhammad Irsyad Abdullah, Management and Science University, Malaysia
Balqees Yaseen Alhaddad, Universiti Geomatika Malaysia, Malaysia

Chapter 7
Navigating Cybersecurity and Privacy in Smart Urban Ecosystems: Challenges, Technologies, and Governance Pathways 189
Syeda Nida Hassan, Ravensbourne University, London, UK

Chapter 8
Safeguarding Urban Intelligence: Redefining IoT Networks With Privacy in Mind 211
G. Mani, University College of Engineering, Kancheepuram, India
J. Rajeshwari, Dayananda Sagar college of Engineering, India
R. Suganthi, Panimalar Engineering College, India
P. Smitha Vas, LBS Institute of Technology for Women, India
G. Manoj Kumar, LBS College of Engineering, India
N. V. Keerthana, Velalar College of Engineering and Technology, India

Chapter 9
Security-as-a-Service: Enhancing Cloud Security Through Managed Security Solutions 239
Zainab Senan Attar Bashi, International Islamic University Malaysia, Malaysia
Azana Hafizah Mohd Aman, Universiti Kebangsaan Malaysia, Malaysia
Salem Sati, Misurata University, Libya
Nur-Adib Maspo, International Islamic University Malaysia, Malaysia
Aisha Hassan Abdalla Hashim, International Islamic University Malaysia, Malaysia

Chapter 10
Solar and Wind Energy in Urban Transformation: Opportunities, Challenges, and Cybersecurity 271
Tamara Phillips Fudge, Purdue University Global, USA
Susan Shepherd Ferebee, Purdue University Global, USA

Chapter 11
The Convergence of Artificial Intelligence and the Internet of Things for Next-Generation Smart Systems 311
G. Swetha, RR Institute of Technology, Bangalore, India
M. S. Veena, RR Institute of Technology, Bangalore, India
Tejaswini Krishnamurthy, RR Institute of Technology, Bangalore, India
S. Druva Kumar, Dayananda Sagar College of Engineering, India
M. Shruthi, Dayananda Sagar College of Engineering, India
S. Vishwanatha, Jain University, India
N. Raghu, Jain University, India
V. N. Trupti, Jain University, India

Chapter 12
The Ethics of Data Collection and Usage in Smart City Infrastructure 337
Zokir Mamadiyarov, Termez University of Economics and Service, Uzbekistan
Barno Matchanova, Urgench State Pedagogical Institute, Uzbekistan
Shokhjakhon Akhmedov, Urgench State University, Uzbekistan
Munir Ahmad, Survey of Pakistan, Pakistan

Chapter 13
The Threat Landscape of Smart Urban Ecosystems: A Survey......................... 371
Mohammad Albadareen, Hashemite University, Jordan
Abdullah Al-Husseaney, Hashemite University, Jordan
Mahmoud Aljawarneh, Applied Science Private University, Jordan
Qais Al-Na'amneh, Applied Science Private University, Jordan
Fadi Batah, Applied Science Private University, Jordan
Ahmad saleh Alhazaimeh, King Abdaulaziz University, Saudi Arabia
Rahaf Hazaymih, Jordan University of Science and Technology, Jordan

Chapter 14
Trust Through Transparency: Blockchain-Enabled Supply Chain Traceability for Smart Urban Ecosystems... 393
Yahaya Saidu, Universiti Teknologi PETRONAS, Malaysia & Taraba State University, Jalingo, Nigeria
Shuhaida Mohamed Shuhidan, Universiti Teknologi PETRONAS, Malaysia
Dahiru Adamu Aliyu, Universiti Teknologi PETRONAS, Malaysia
Suwaiba Siuto Adamu, Taraba State University, Jalingo, Nigeria
Jameel Shehu Yalli, Universiti Teknologi PETRONAS, Malaysia
Hussaini Mamman, Universiti Teknologi PETRONAS, Malaysia

Conclusion 431

Compilation of References 433

About the Contributors 495

Index... 507

Preface

The dawn of the 21st century has witnessed an extraordinary transformation in the way urban environments function, driven by a stream of digital technologies, interconnected devices, and intelligent systems. Smart urban ecosystems are no longer a future concept; they are here, reshaping the foundation of city life. This book, Navigating Cybersecurity and Privacy in the Evolution of Smart Urban Ecosystems, addresses the critical intersection of technology, security, and privacy within the rapidly evolving smart cities. It offers a complete exploration of both the substantial opportunities and extreme challenges inherent in these complex socio-technical systems.

Smart urban ecosystems represent the merging of information and communication technologies (ICT), the Internet of Things (IoT), artificial intelligence (AI), and data analytics with traditional urban infrastructure. This integration enables cities to optimize resources, enhance sustainability, improve governance, and deliver better services to citizens. However, this transformation also exposes urban environments to novel cybersecurity threats and privacy risks, which, if left unchecked, can undermine public trust, disrupt essential services, and compromise urban safety.

The book's focus is to navigate this dynamic environment by providing multidisciplinary perspectives on securing smart cities, ensuring privacy protections, promoting ethical frameworks, and developing resilient governance structures. Through comprehensive chapters contributed by experts, it synthesizes emerging research, practical methodologies, and future-proof strategies to guide readers in understanding and addressing the cyber-physical vulnerabilities that cities of the future will undoubtedly face.

As urban populations grow and cities become more dependent on digital technologies, the stakes for cybersecurity and privacy have never been higher. Critical infrastructure — from energy grids and water management to transportation and public safety — is increasingly automated and interconnected. Global trends such as climate change, urbanization, and technological innovation create a complex environment in which security threats are increasingly sophisticated and privacy concerns are paramount.

In this context, cybersecurity becomes a fundamental support of the smart city's strength. Protecting data integrity, system availability, and citizen privacy is essential not only for maintaining operational continuity but also for fostering civic engagement and democratic governance. Equally important is addressing ethical dilemmas that arise from AI-driven decision-making, surveillance, and data sharing, making it imperative to develop frameworks that balance innovation with responsibility.

This book positions itself as a timely response to these challenges, offering insights into advanced technologies such as blockchain for decentralized security, AI for automation and defense, sensor optimization for urban monitoring, and green cybersecurity practices. It also examines the governance pathways necessary to coordinate stakeholders to achieve secure, transparent, and equitable smart urban ecosystems.

This publication is designed for a diverse audience, including cybersecurity researchers, urban planners, IT professionals, academic educators, and graduate students specializing in smart cities, digital forensics, network security, and urban governance. Practitioners involved in designing, implementing, or regulating smart city infrastructure and digital services will find practical frameworks and case studies relevant to their work.

Additionally, the book aims to update interdisciplinary scholars interested in the socio-technical implications of urban digital transformation. By bridging technical and ethical domains, it invites readers to critically engage with issues of bias, transparency, privacy, and resilience in the context of evolving urban environments. This makes it a valuable resource for advancing both academic scholarship and practical implementation.

The following chapters outline the key themes and concepts explored in this book:

CHAPTER 1: AN OVERVIEW OF SMART CITIES COVERING APPLICATIONS, CHALLENGES, AND EMERGING TRENDS

This foundational chapter introduces readers to the core concepts, technologies, and drivers of smart cities. It frames the overall discourse by identifying key applications, persistent challenges, and the innovative trends that define ongoing urban transformation.

CHAPTER 2: WHEN NATURE MEETS CODE: GOVERNING GREY DATA FOR CYBERSECURITY AND SUSTAINABILITY SMART CITIES

This chapter examines the governance of “grey data” — ambiguous or partially structured data —highlighting its dual role in cybersecurity and environmental sustainability. It emphasizes the importance of managing data ecosystems carefully to achieve both secure and sustainable urban operations.

CHAPTER 3: BLOCKCHAIN BEYOND CRYPTOCURRENCY - -- A DECENTRALIZED APPROACH TO URBAN SECURITY

The chapter highlights integration hurdles such as interoperability, regulatory gaps, and ethical tensions, while outlining emerging trends like Blockchain 4.0, quantum-safe cryptography, and DAO-led civic participation. It offers a roadmap for decentralized citizen-centric governance in smart cities.

CHAPTER 4: CYBERATTACKS BLOCKCHAIN BEYOND CRYPTOCURRENCY A DECENTRALIZED APPROACH TO URBAN SECURITY

This chapter investigates trends in cyberattacks targeting blockchain implementations in smart urban settings, analyzing vulnerabilities and defenses to strengthen trust in decentralized mechanisms.

CHAPTER 5: CYBERSECURITY AT THE EDGE DEFENDING DECENTRALIZED CITIES IN A BORDERLESS THREAT LANDSCAPE

Focusing on edge computing, this chapter addresses security paradigms for decentralized networks critical to smart cities, offering insights into protecting distributed assets in an increasingly borderless cyberthreat environment.

CHAPTER 6: ENHANCING CYBERSECURITY, PRIVACY INNOVATION AND E-GOVERNMENT READINESS IN SMART CITIES: A FRAMEWORK FOR AWARENESS AND RESILIENCE

This contribution proposes a comprehensive framework to boost cybersecurity knowledge, privacy innovation, and governmental preparedness to build resilience against cyber threats specific to E-governance contexts.

CHAPTER 7: NAVIGATING CYBERSECURITY AND PRIVACY IN SMART URBAN ECOSYSTEMS CHALLENGES, TECHNOLOGIES, AND GOVERNANCE PATHWAYS

Resilience is key to enduring cyber disruptions. This chapter articulates principles and methods for designing robust smart urban systems capable of rapid recovery and sustained, secure operation despite adversities.

CHAPTER 8: SAFEGUARDING URBAN INTELLIGENCE-REDEFINING IOT NETWORKS WITH PRIVACY IN MIND: IOT FOR URBAN SYSTEMS

IoT devices are extensively integrated into modern systems, but their security vulnerabilities create significant challenges. This chapter proposes privacy-centric design and security solutions to safeguard urban IoT deployments, protecting citizen data while enabling smart functionalities.

CHAPTER 9: SECURITY-AS-A-SERVICE: ENHANCING CLOUD SECURITY THROUGH MANAGED SECURITY SOLUTIONS

Cloud computing supports many smart city platforms. This chapter explains how security-as-a-service models provide scalable, managed protection to cloud infrastructures against evolving cyber threats.

CHAPTER 10: SOLAR AND WIND ENERGY IN URBAN TRANSFORMATION: OPPORTUNITIES, CHALLENGES, AND CYBERSECURITY

Renewable energy integration into urban grids introduces unique cybersecurity demands. This chapter discusses securing solar and wind infrastructure against cyber threats while leveraging their environmental benefits.

CHAPTER 11: THE CONVERGENCE OF ARTIFICIAL INTELLIGENCE AND THE INTERNET OF THINGS FOR NEXT-GENERATION SMART SYSTEMS

This chapter explores the integration of AI and IoT as core technologies for next-generation urban systems. It highlights their combined role in enhancing security and privacy. Additionally, it examines how this synergy improves operational intelligence in smart cities.

CHAPTER 12: THE ETHICS OF DATA COLLECTION AND USAGE IN SMART CITY INFRASTRUCTURE

Data is central to smart cities but raises ethical questions. This chapter critically analyzes ethical frameworks guiding responsible data collection, consent, and usage in urban environments.

CHAPTER 13: THE THREAT LANDSCAPE OF SMART URBAN ECOSYSTEMS-A SURVEY

This chapter provides a systematic overview of both current and emerging cyber threats facing urban ecosystems. It explores the motivations behind these attacks and identifies common vulnerabilities. Additionally, it presents practical strategies to defend against such threats.

CHAPTER 14: TRUST THROUGH TRANSPARENCY-BLOCKCHAIN-ENABLED SUPPLY CHAIN TRACEABILITY FOR SMART URBAN ECOSYSTEMS

Supply chains are essential parts of urban systems, but they are also exposed to various risks and vulnerabilities. This chapter discusses how blockchain enhances transparency and trustworthiness in urban supply chains.

Chapter 9

Security-as-a-Service:
Enhancing Cloud Security Through Managed Security Solutions

Zainab Senan Attar Bashi
https://orcid.org/0000-0002-1452-8098
International Islamic University Malaysia, Malaysia

Azana Hafizah Mohd Aman
https://orcid.org/0000-0001-7337-6736
Universiti Kebangsaan Malaysia, Malaysia

Salem Sati
https://orcid.org/0000-0002-6062-497X
Misurata University, Libya

Nur-Adib Maspo
https://orcid.org/0000-0003-0031-1354
International Islamic University Malaysia, Malaysia

Aisha Hassan Abdalla Hashim
https://orcid.org/0000-0001-6331-1373
International Islamic University Malaysia, Malaysia

ABSTRACT

Cloud computing plays an important role in modern businesses by enabling flexible, efficient storage, analysis, and access to data and applications. However, this reliance also introduces new security challenges. Ensuring cloud security and resilience is now critical to prevent unauthorized access, data breaches, and service disruptions. This chapter examines the key principles, technologies, and policies that uphold the confidentiality, integrity, and availability of cloud systems.

DOI: 10.4018/979-8-3373-4455-3.ch009

It also highlights Security-as-a-Service (SECaaS) as a necessary part of the cloud ecosystem, offering specialized, scalable solutions to improve overall security. By delivering managed security services via the cloud, SECaaS allows organizations to outsource key functions such as threat intelligence, endpoint protection, access control, and compliance monitoring. It can enhance protection without heavy in-house investment

1. INTRODUCTION

In the era of digital transformation, cloud computing has become the backbone of modern business operations, offering unparalleled scalability, operational flexibility, and innovative capabilities (Kaluvuri et al., 2015). The migration to cloud environments allows enterprises to operate at a global scale, collaborate seamlessly, and use data-driven insights to remain competitive. However, this transition introduces a spectrum of security challenges that cannot be ignored, such as data breaches, unauthorized access, and compliance risks (Mostafa et al., 2023). These challenges arise due to the dynamic and interconnected nature of cloud networks, which demand robust and adaptive security mechanisms. Security-as-a-Service (SECaaS) has emerged as a vital solution, addressing these challenges by providing managed security services tailored to the unique demands of cloud-based infrastructures (Shen et al., 2013).

SECaaS revolutionizes the way organizations handle security by shifting the burden from internal IT teams to specialized service providers. This approach allows businesses to concentrate on their core operations while using advanced security tools and expertise from external providers. SECaaS embodies the principles of resilience, scalability, and real-time responsiveness, delivering comprehensive protection against an evolving threat landscape.

One of the core strengths of SECaaS lies in its ability to implement proactive security measures that safeguard cloud infrastructures (Talib et al., 2012). These measures include vulnerability scanning, penetration testing, and continuous monitoring (Casola et al., 2018), which are necessary for identifying and mitigating potential security weaknesses. Wang & Shen (2013) highlight the effectiveness of services like CloudProxy, which operate within network architectures to detect vulnerabilities in real time. Such tools act as intermediaries between clients and cloud services, scanning traffic flows and application layers for anomalies that may signal potential breaches.

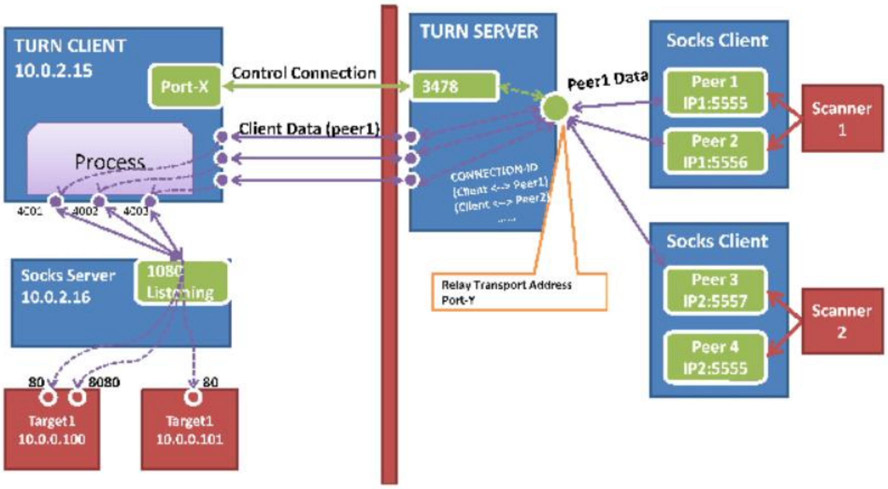

Figure 1. Overall Structure of CloudProxy (Wang & Shen, 2013)

By incorporating tools like intrusion detection systems (IDS) and intrusion prevention systems (IPS), SECaaS providers enhance network-level security (Rullo et al., 2024). These systems analyze traffic patterns using predefined rules or machine learning algorithms to identify malicious activities, such as distributed denial-of-service (DDoS) attacks or data exfiltration attempts. Table 1 summarizes some of the researches about ML algorithms used in IPS and IDS. Furthermore, the integration of secure communication protocols, such as Transport Layer Security (TLS), ensures that data traversing cloud networks is encrypted, maintaining confidentiality and integrity.

Table I. Machine Learning for IDS and IPS

References	Algorithm	Type	Typical Use in IPS/IDS	Advantages	Limitations
(R. Tahri et al., 2024; Yang et al., 2019)	Decision Tree (DT)	Supervised	- Used for both IPS and IDS - Signature-based or anomaly detection	- Easy to interpret and implement - Fast training - Handles small datasets well	- Prone to overfitting when dealing with complex data - May require pruning or ensemble methods for improved accuracy
(Jayshree & Leena, 2013; Su et al., 2021)	Support Vector Machine (SVM)	Supervised	- Commonly used in IDS - Can be extended for IPS with relevant kernel functions	- High classification accuracy - Effective in high-dimensional spaces - Good for smaller datasets	- Parameter tuning (kernel selection, C, gamma) can be complex - Slower training for large datasets
(Awotunde et al., 2023; Farnaaz & Jabbar, 2016)	Random Forest (RF)	Supervised	- Used in both IDS (signature & anomaly) and IPS - Effective for high-dimensional network traffic data	- More robust to overfitting compared to single DT - High accuracy - Can handle missing values	- Less interpretable than a single decision tree - Training can be slower than simple DT methods
(Awotunde et al., 2023; Mukherjee & Sharma, 2012)	Naive Bayes (NB)	Supervised	- Commonly used for IDS classification - Works well for textual or log-based detection	- Fast training - Simple to implement - Effective with small datasets	- Assumes feature independence - Lower accuracy if strong dependencies exist among features
(Lakshminarayana & Basarkod, 2023; Nikhitha & Jabbar, 2019)	K-Nearest Neighbor (KNN)	Supervised (Instance-Based)	- Often used in IDS for anomaly detection - Helps detect rare intrusions	- Conceptually simple - Can achieve good accuracy with small-to-medium datasets - Non-parametric	- High computational cost during inference - Sensitive to noise and irrelevant features

(Aljuaid & Alshamrani, 2024; Hnamte & Hussain, 2023; Khan et al., 2022)	Deep Learning (DL) (e.g., CNN, RNN)	Supervised or Unsupervised (depending on architecture)	- Used in both IDS and IPS - Excels in anomaly detection and feature extraction in high-volume network traffic	- Automated feature extraction - Highly accurate for complex data patterns - Can handle large-scale inputs	- Requires large labeled datasets - High computational and memory requirements - Model interpretability can be challenging

While the use of ML algorithms in intrusion detection and prevention systems within SECaaS environments has been widely studied, much of the existing literature highlights ongoing trade-offs that remain unresolved (Shirley C P et al., 2025). For example, algorithms such as Support Vector Machines (SVM) and Random Forests often achieve high detection accuracy but impose significant computational overhead, making them less suitable for real-time applications in resource-constrained cloud environments. By contrast, lightweight models such as k-Nearest Neighbors (kNN) or Naïve Bayes reduce complexity but often sacrifice accuracy, especially when dealing with zero-day attacks or highly imbalanced datasets. Another key trade-off lies in the choice between supervised and unsupervised learning approaches. While supervised models generally achieve higher precision given labelled datasets, they struggle with scalability and adaptability in dynamic cloud infrastructures where labelled attack data may not be readily available. Unsupervised approaches, such as clustering or anomaly detection methods, offer adaptability to unknown attack vectors but typically generate higher false-positive rates, which can overwhelm security operations teams. Similarly, deep learning methods such as Convolutional Neural Networks (CNNs) and Deep Residual Networks (DRNs) show strong performance in complex pattern recognition, yet they demand significant training data and high computational resources, raising questions about their practicality in real-time SECaaS deployments.

Beyond these algorithmic trade-offs, several open challenges persist in applying ML-driven IDS/IPS to SECaaS. Scalability in multi-cloud environments remains a pressing issue (Stephenson Achankeng, 2025), as distributed workloads require models that can operate consistently across heterogeneous platforms while maintaining low latency. Moreover, the rise of adversarial ML threats poses risks to IDS/IPS reliability, as attackers can manipulate input data to evade detection or trigger false alarms. This vulnerability underscores the need for more robust and explainable AI approaches in security. Additionally, achieving real-time deployment is a challenge, as high-performing ML models often require extensive preprocessing and inference time, creating delays that undermine the immediate response capability expected from SECaaS solutions. These challenges suggest that while ML offers powerful tools for IDS/IPS, its current application in SECaaS is not without limitations. Future research must therefore focus on developing lightweight, adaptive, and adversarial-resistant algorithms that balance accuracy with operational feasibility in distributed, high-demand cloud environments.

On the other hand, the rise of multi-agent systems (MAS) has transformed how security is managed in collaborative cloud environments (Fedele et al., 2025). These systems use autonomous agents distributed across the network to perform security tasks such as monitoring, access control, and anomaly detection. (Talib et al., 2012) demonstrate that MAS can seamlessly manage security across distributed storage systems, ensuring the confidentiality, integrity, and availability of data. MAS provides decentralized and adaptive security measures that are essential for managing complex and dynamic cloud infrastructures.

MAS agents communicate and collaborate using standardized protocols, enabling a complete view of the network's security posture as in Figure 2. For example, agents deployed at various nodes of a cloud network can detect local threats and share intelligence with other agents to coordinate responses. This decentralized approach minimizes the risk of single points of failure, a critical consideration in distributed systems. Engineers must design these agents to be lightweight, efficient, and capable of operating in resource-constrained environments, such as edge devices and mobile platforms.

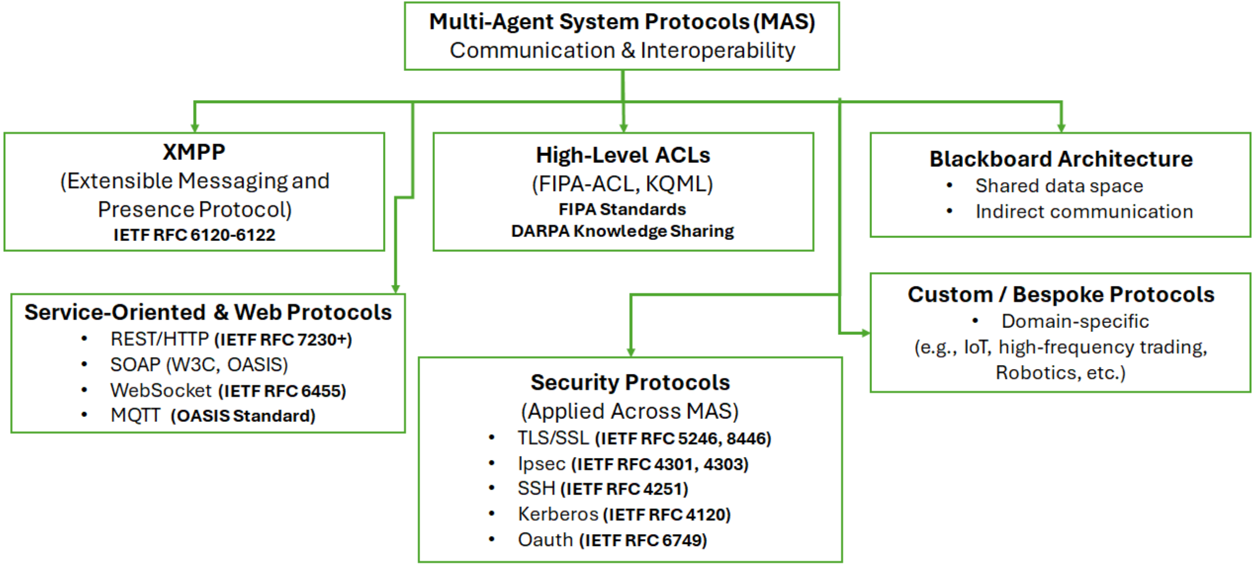
Multi-Agent System Protocols (MAS)
Communication & Interoperability
XMPP
(Extensible Messaging and Presence Protocol)
IETF RFC 6120-6122
High-Level ACLs
(FIPA-ACL, KQML)
FIPA Standards
DARPA Knowledge Sharing
Blackboard Architecture
• Shared data space
• Indirect communication
Service-Oriented & Web Protocols
• REST/HTTP (IETF RFC 7230+)
• SOAP (W3C, OASIS)
• WebSocket (IETF RFC 6455)
• MQTT (OASIS Standard)
Custom / Bespoke Protocols
• Domain-specific
(e.g., IoT, high-frequency trading, Robotics, etc.)
Security Protocols
(Applied Across MAS)
• TLS/SSL (IETF RFC 5246, 8446)
• Ipsec (IETF RFC 4301, 4303)
• SSH (IETF RFC 4251)
• Kerberos (IETF RFC 4120)
• Oauth (IETF RFC 6749)

Figure 2. Protocols and Standards related to MAS

As mobile cloud computing (Asghari & Sohrabi, 2024)gains traction, securing these environments has become a top priority. Mobile devices frequently access cloud services over untrusted networks, making them susceptible to threats such as man-in-the-middle attacks and unauthorized access. Jafari et al. (2016) propose frameworks designed to address these unique challenges while maintaining user convenience. These frameworks integrate robust authentication mechanisms, such as multifactor authentication (MFA) and biometric verification, to enhance access control.

In addition to authentication, secure communication channels play a critical role in protecting mobile cloud interactions. Techniques such as end-to-end encryption and secure tunnelling protocols (e.g., Virtual Private Networks) ensure that data transmitted between mobile devices and cloud servers remains confidential. It is important to consider high variability of mobile environments, optimizing security solutions for low-latency and high-throughput scenarios to provide a seamless user experience.

Beyond traditional threats, organizations are increasingly confronted with advanced persistent threats (APTs), which are highly targeted, prolonged cyberattacks designed to compromise sensitive systems (Yuan et al., 2020). To counter such threats, SECaaS providers are incorporating advanced defense strategies, including game-theory-based models. Yuan et al. (2020) discuss the application of Stackelberg-game-based strategies in cloud security, where defenders and attackers engage in a simulated game to predict and mitigate potential attack vectors.

In a Stackelberg framework, SECaaS providers act as leaders, deploying defensive strategies based on anticipated attacker behavior. This approach requires extensive data collection and analysis to model the attacker's objectives, resources, and methods. A real-time telemetry and analytics pipelines, which feed critical data into the game-theory algorithms should be implemented. These models help prioritize security measures, such as patching high-risk vulnerabilities and deploying decoy systems to misdirect attackers.

Leading providers such as AWS Security Hub, Microsoft Defender for Cloud, and Google Cloud Security Command Center offer overlapping yet distinct service portfolios. For example, AWS emphasizes compliance automation and continuous monitoring, while Microsoft integrates advanced AI-driven analytics into identity and access management. Google, on the other hand, uses its global infrastructure to provide scalable threat intelligence and rapid response capabilities. These differences illustrate how provider selection can shape an organization's security strategy, influencing costs, interoperability, and performance.

Meeting regulatory and industry compliance standards is a critical requirement for organizations operating in the cloud. Regulations such ISO/IEC 27001 (Information Security Management Systems), CSA STAR (Security, Trust & Assurance Registry), and Health Insurance Portability and Accountability Act (HIPAA) impose stringent requirements on data protection and privacy (see Figure 3). SECaaS simplifies compliance with industry standards by automating monitoring and reporting processes, reducing the administrative burden on businesses.

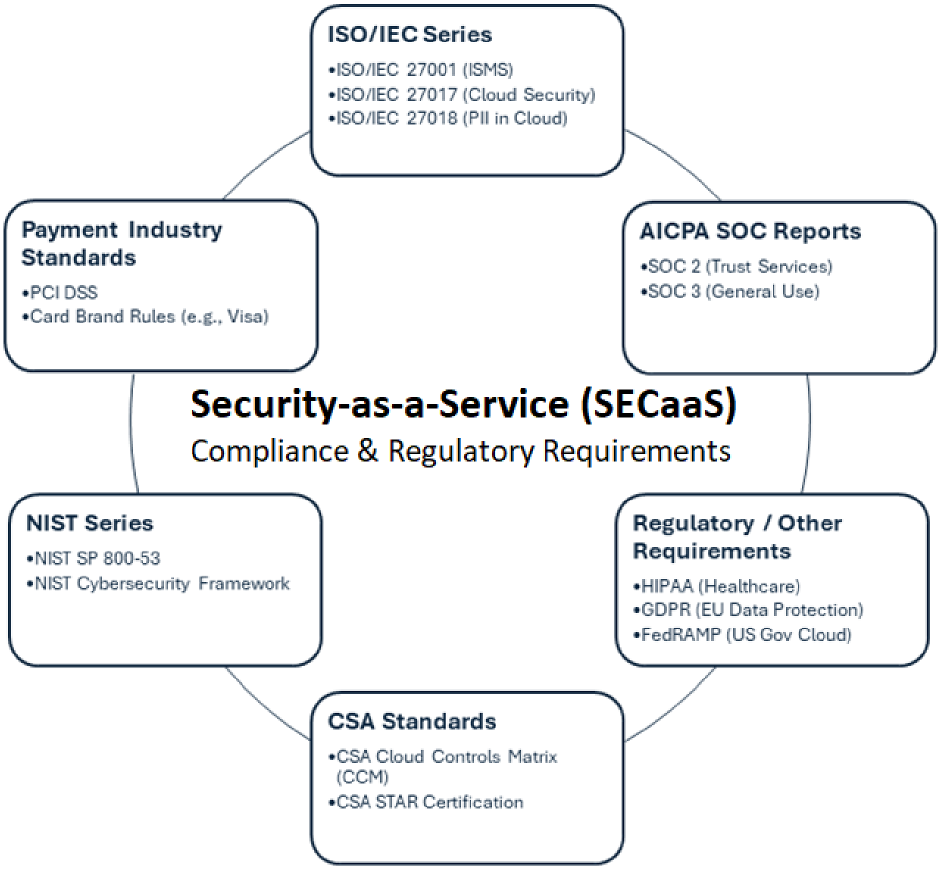
ISO/IEC Series
•ISO/IEC 27001 (ISMS)
•ISO/IEC 27017 (Cloud Security)
•ISO/IEC 27018 (PII in Cloud)
Payment Industry Standards
•PCI DSS
•Card Brand Rules (e.g., Visa)
AICPA SOC Reports
•SOC 2 (Trust Services)
•SOC 3 (General Use)
Security-as-a-Service (SECaaS)
Compliance & Regulatory Requirements
NIST Series
•NIST SP 800-53
•NIST Cybersecurity Framework
Regulatory / Other Requirements
•HIPAA (Healthcare)
•GDPR (EU Data Protection)
•FedRAMP (US Gov Cloud)
CSA Standards
•CSA Cloud Controls Matrix (CCM)
•CSA STAR Certification

Figure 3. SECaaS Compliance and Regulatory Requirements

Automation involves integrating SECaaS solutions with compliance frameworks to continuously monitor data flows, access controls, and system configurations. For instance, cloud-based Security Information and Event Management (SIEM) systems aggregate logs from across the network, analyzing them for compliance violations and generating reports for auditors. These systems should be designed to handle high volumes of data, ensuring real-time analysis and alerting capabilities.

SECaaS providers need to adopt advanced technologies to enhance their offerings. These technologies include:

1. **Machine Learning and Artificial Intelligence (AI):** ML and AI algorithms analyze huge datasets to detect subtle patterns indicative of cyber threats (Muneer et al., 2024). For example, anomaly detection models identify deviations from normal traffic behavior, flagging potential attacks.
2. **Blockchain for Security Transparency:** Blockchain-based solutions provide immutable audit trails, ensuring accountability in security operations (Jurgała et al., 2022). Integrating blockchain in the systems can enhance trust and traceability within distributed cloud networks.
3. **Zero Trust Architectures:** Zero Trust models enforce strict verification of every user and device attempting to access network resources (García-Teodoro et al., 2022). This approach minimizes the risk of insider threats and lateral movement within cloud systems.
4. **Edge Computing Integration:** As edge computing becomes more prevalent, SECaaS solutions are extending their reach to protect data and devices at the network's edge (Ranaweera et al., 2020). Lightweight agents and secure gateways are deployed to ensure end-to-end protection.

The adoption of SECaaS is not merely a cost-saving measure but a strategic move to enhance organizational resilience in an increasingly hostile cyber landscape. By offloading security responsibilities to specialized providers, businesses gain access to expertise and resources that would be prohibitively expensive to develop in-house. Furthermore, SECaaS solutions are inherently scalable, adapting to the evolving needs of organizations as they grow and expand their cloud operations. SECaaS represents an opportunity to collaborate with providers in designing, deploying, and optimizing security solutions that align with organizational goals.

2. The Fundamentals of Security-as-a-Service

The rise of Security-as-a-Service (SECaaS) marks a significant evolution in how organizations approach cybersecurity, offering scalable, cost-effective, and adaptive solutions built to the rapidly changing threat landscape. Unlike traditional on-premises security models that rely on dedicated hardware and extensive in-house expertise, SECaaS delivers security services through cloud infrastructure on a subscription basis. This shift allows businesses to use advanced tools and expertise without incurring the high costs associated with developing and maintaining such capabilities internally.

At its core, SECaaS is an outsourcing model in which security services are hosted and managed in the cloud, providing comprehensive protection to businesses. As described by Wang & Shen (2013), SECaaS includes critical functionalities such as vulnerability scanning, penetration testing, and real-time threat monitoring. These services are designed to be adaptive, responding to emerging threats with minimal latency.

This model's dynamic nature allows organizations to benefit from cutting-edge security solutions that might otherwise be financially or technically infeasible. For instance, SECaaS providers continuously update their systems with the latest threat intelligence, ensuring that businesses remain protected against evolving cyber threats. Unlike traditional models, which rely on periodic manual updates, SECaaS automates these processes, reducing the risk of human error and ensuring up-to-date defences.

SECaaS addresses several limitations of traditional on-premises security solutions by offering a range of advantages that are particularly appealing from a networking and security engineering perspective:

1. Scalability: SECaaS solutions are highly scalable, capable of adjusting to the fluctuating demands of modern organizations. Whether managing small-scale systems or complex multi-cloud environments, SECaaS adapts to workload changes seamlessly, avoiding the infrastructure constraints inherent in traditional models (Elsayed & Zulkernine, 2019).
2. Cost-Effectiveness: By eliminating the need for upfront capital expenditures on hardware and in-house expertise, SECaaS reduces operational costs. Subscription-based pricing models allow organizations to pay for services based on usage, making high-quality security accessible even to small and medium-sized enterprises (SMEs).
3. Real-Time Threat Intelligence: SECaaS uses global threat intelligence networks to provide real-time updates. This continuous flow of intelligence enhances the system's ability to detect and mitigate threats as they arise, a stark contrast to the delayed updates typical in traditional systems.
4. Ease of Deployment and Maintenance: Cloud-based deployment ensures rapid integration of security services, often without disrupting existing workflows. Maintenance is managed by the service provider, including automatic updates and patches, easing the burden on internal IT teams.
5. Flexibility and Accessibility: SECaaS solutions are designed to support hybrid and multi-cloud environments, ensuring seamless integration across various platforms. Additionally, they are accessible from anywhere, facilitating security management in globally distributed networks (Fehis et al., 2021).
6. Enhanced Compliance Management: Built-in compliance tools simplify audits and reporting, helping organizations adhere to regulatory standards such as GDPR and HIPAA. This feature reduces the administrative burden on IT staff and minimizes the risk of non-compliance penalties.

The core components of SECaaS are integral to its success. These components encompass a wide array of security functions designed to provide comprehensive protection for modern IT infrastructures:

1. Identity and Access Management (IAM): IAM systems within SECaaS ensure that only authorized users can access cloud resources. By integrating multi-factor authentication (MFA), single sign-on (SSO), and user behavior analytics, these systems strengthen identity verification processes (Fehis et al., 2021).
2. Intrusion Detection and Prevention Systems (IDPS): Real-time detection and prevention of malicious activities are fundamental to SECaaS. Advanced IDPS frameworks, such as those highlighted by Sharma et al. (2016), monitor network traffic for suspicious patterns. Using machine learning algorithms, these systems can identify zero-day exploits and respond automatically, reducing reliance on manual intervention.
3. Data Loss Prevention (DLP): DLP solutions protect sensitive data from unauthorized access or accidental leaks. These systems monitor data flows, enforce encryption policies, and block suspicious transfers (Sharma et al., 2016).
4. Endpoint Protection: With the spread of mobile and IoT devices, endpoint protection has become a priority. SECaaS extends security measures to all connected devices, providing antivirus, anti-malware, and patch management solutions.
5. Web Application Firewalls (WAFs): Web applications hosted in the cloud are frequent targets for attacks such as SQL injection and cross-site scripting (XSS). WAFs filter and monitor HTTP requests to identify and block malicious traffic (Hashizume et al., 2013).

6. Advanced Persistent Threat (APT) Defence: Combating APTs requires sophisticated strategies. Yuan et al. (2020) emphasize game-theory-based approaches, such as Stackelberg strategies, which simulate attacker-defender interactions to anticipate and counteract threats. Security engineers use these models to design proactive defence mechanisms.

Table 2 below highlights the differences between SECaaS and traditional on-premises security solutions:

Table II. Differences between SECaaS and traditional Security Models

Feature	SECaaS	Traditional Security Models
Scalability	Adapts to changing workloads and organizational needs.	Limited by hardware and infrastructure capacity.
Cost-Effectiveness	Subscription-based, reducing capital expenditures.	High initial costs for hardware and maintenance.
Real-Time Threat Intelligence	Continuous updates and global intelligence networks.	Relies on periodic updates and lacks real-time insights.
Ease of Deployment	Rapid deployment via cloud.	Time-intensive setup requiring significant effort.
Maintenance	Provider-managed updates and patches.	Requires in-house IT staff for maintenance.
Flexibility	Supports hybrid and multi-cloud integration.	Challenging to integrate with other systems.
Compliance Management	Automated tools simplify audits and reporting.	Manual compliance monitoring is resource-intensive.
Threat Detection	Real-time detection with automated responses.	Slower manual response times.
Accessibility	Accessible from anywhere via the internet.	Restricted to physical infrastructure locations.

Some of the SECaaS networking and security design considerations are:

1. Architectural Design: Integrating SECaaS into existing IT environments requires a thorough understanding of architectural principles. Cloud-based security tools should interoperate seamlessly with on-premises systems, hybrid networks, and edge devices.
2. Traffic Optimization: SECaaS solutions must analyze network traffic without introducing significant latency. Traffic flows can be optimized using content delivery networks (CDNs), load balancers, and traffic shaping techniques (Chaisiri et al., 2015).
3. Resilience and Redundancy: Cloud-based security services must be designed for high availability. Redundancy mechanisms, such as failover systems and backup data centres, ensure uninterrupted service during outages.
4. Risk Management: Potential risks, such as vendor lock-in and data sovereignty concerns should be evaluated. By selecting flexible providers and implementing localized controls, organizations can mitigate these risks effectively.
5. Automation and Orchestration: Automation plays a crucial role in SECaaS, from compliance monitoring to incident response (Settanni et al., 2023a). Tools should be integrated seamlessly into existing workflows, reducing manual overhead.

3. How SECaaS Enhances Cloud Security

One of the most critical features of SECaaS is its ability to proactively identify and neutralize security risks before they can cause significant damage. This proactive approach is enabled by advanced technologies such as vulnerability scanning and penetration testing, which are delivered through cloud-based proxies. As noted by Genge et al. (2015) these tools provide organizations with real-time detection capabilities, allowing them to address vulnerabilities immediately.

Vulnerability scanning involves examining network components, such as firewalls, routers, and endpoints, to identify weaknesses. Penetration testing simulates potential attacks to evaluate the resilience of these systems. By using cloud resources, SECaaS providers can perform these tasks at scale, delivering detailed reports that inform corrective actions. This ensures that organizations are equipped to neutralize potential threats promptly, reducing the risk of data breaches and minimizing downtime.

In addition to basic detection tools, SECaaS solutions incorporate advanced persistent threat (APT) defences. Srinadh et al. (2023) highlight a Conditional Dingo Optimization Algorithm (CDOA) combined with a Deep Residual Network (DRN) to detect Advanced Persistent Threats (APTs). While Moving Target Defense (MTD) mitigates APTs by shifting attack surfaces, it often incurs high overhead.

1) Scalability and Flexibility in Security Management

Modern networking environments, especially those operating in hybrid or multi-cloud setups, demand flexible security solutions. SECaaS provides unparalleled scalability, enabling organizations to adjust their security measures dynamically based on workload fluctuations. Unlike traditional security systems, which require substantial capital investment and infrastructure upgrades to scale, SECaaS offers on-demand scalability without the need for additional hardware.

2) Real-Time Monitoring and Automated Response

Real-time monitoring is a cornerstone of SECaaS, enabling organizations to detect and respond to threats as they occur. Systems design should continuously analyze network traffic, identifying anomalies that may indicate malicious activity. These systems use techniques such as deep packet inspection (DPI) and behavioural analysis to examine data flows, ensuring that threats are detected at the earliest stages (Ashraf et al., 2016).

Automated response mechanisms are another critical aspect of SECaaS. Once a threat is detected, these systems can initiate predefined actions, such as isolating compromised devices, blocking malicious IP addresses, or alerting security teams. This automation significantly reduces response times, limiting the potential impact of attacks (Settanni et al., 2023b).

3) Comprehensive Data Protection

In cloud computing, data protection is paramount, as sensitive information is often stored and transmitted across distributed networks. SECaaS addresses this challenge by providing robust data protection mechanisms, such as data loss prevention (DLP) and encryption. DLP solutions monitor data flows within the network, identifying and blocking unauthorized transfers of sensitive information.

Encryption is another essential component of SECaaS. By securing data during both transmission and storage, encryption ensures confidentiality and integrity. Networking engineers implement encryption protocols, such as Transport Layer Security (TLS) and IPsec, to protect data traveling across public and private networks. Additionally, they manage encryption key lifecycles, ensuring that keys are securely stored, rotated, and retired.

Intelligent algorithms and automated workflows enforce strict access controls, ensuring that only authorized users can access sensitive data.

4) Enhanced Collaboration and Integration

In complex cloud ecosystems, collaboration and integration are critical to ensuring comprehensive security. SECaaS solutions facilitate seamless coordination among various security components, creating a unified defence strategy. All security components should be configured to communicate effectively, using standardized protocols such as Syslog and SNMP for logging and monitoring. Integration also involves centralizing security management through platforms such as Security Information and Event Management (SIEM) systems, which aggregate data from across the network and provide a comprehensive view of the security posture.

While SECaaS offers significant advantages, its implementation also presents unique challenges:

1) *Latency and Performance:* Real-time monitoring and automated responses must be optimized to avoid introducing latency that could impact network performance. Some of the techniques to be used are load balancing and edge computing to distribute processing workloads and maintain responsiveness.
2) *Data Sovereignty and Privacy:* Organizations must ensure that SECaaS solutions comply with data sovereignty regulations, which may restrict where data can be stored and processed. Localized data centres and region-specific configurations should be implemented to address these requirements. Addressing data sovereignty involves implementing robust data routing and geo-fencing solutions. Data packets originating in specific jurisdictions should remain within compliant data centers, using technologies such as software-defined networking (SDN) to enforce location-based routing policies. Furthermore, encryption protocols, such as Transport Layer Security (TLS) and end-to-end encryption, should be used to secure data during transit.
3) *Integration Complexity:* Integrating SECaaS with legacy systems and hybrid cloud environments can be challenging. Solutions should be built to bridge gaps between traditional and modern architectures, ensuring interoperability and consistency.
4) *Vendor Lock-In:* Relying exclusively on a single Security-as-a-Service (SECaaS) provider can limit an organization's flexibility, making it more difficult and costly to switch vendors if performance, pricing, or strategic needs evolve. This situation, often referred to as "vendor lock-in," restricts an organization's negotiation power and ability to adopt innovative solutions from other providers. To mitigate this risk, networking engineers must prioritize SECaaS providers that adhere to open standards and support interoperable architectures. For example, providers offering services based on RESTful APIs, OpenConfig, or Common Information Model (CIM) facilitate seamless integration with diverse systems. Additionally, modular network architectures can be implemented to allow components, such as firewalls or intrusion detection systems (IDS), to be replaced without impacting the overall security posture.

5) *Reliability and Service-Level Agreements (SLAs):* The reliability of SECaaS solutions is directly tied to the stability and performance of the provider's infrastructure. Downtime, outages, or service disruptions can have severe consequences for organizational security, including increased vulnerability to cyberattacks. Key elements to consider in SLAs include:

- Uptime Guarantees: Providers should offer clear commitments, such as 99.9% availability, backed by penalties for non-compliance.
- Incident Response Times: SLAs should specify response times for threat detection, containment, and remediation.

- Disaster Recovery Provisions: Engineers must verify the existence of failover systems, redundant data centers, and recovery point objectives (RPOs) that align with organizational needs.

6) *Regulatory Compliance:* Cloud environments are dynamic and complex, often complicating adherence to regulatory and industry standards. While SECaaS providers offer compliance tools and certifications, ultimate responsibility for regulatory adherence typically remains with the client. Key strategies include:
   - Centralized Compliance Dashboards: SIEM (Security Information and Event Management) systems can be integrated with centralize compliance monitoring, automating the detection of non-compliance issues.
   - Encryption Standards: Implementing encryption for data at rest and in transit helps meet stringent data protection requirements.
   - Segmentation and Access Controls: Using network segmentation and zero-trust architectures, engineers can isolate sensitive data and restrict access based on roles.
7) *Integration Complexity:* Integrating SECaaS solutions into existing IT infrastructures, particularly in hybrid or multi-cloud environments, presents significant challenges. Legacy systems often lack compatibility with modern cloud-based services, requiring substantial engineering efforts to bridge the gap. Integration involves:
   - Assessing Compatibility: existing hardware, software, and protocols should be evaluated to identify potential integration issues.
   - Implementing Gateways and Adapters: API gateways and protocol converters can enable communication between legacy systems and SECaaS platforms.
   - Standardized Network Architectures: Adopting standards such as VXLAN (Virtual Extensible LAN) or IPv6 can simplify integration and ensure scalability (Conrad et al., 2023).
8) *Cost Management:* While SECaaS is often praised for its cost-efficiency, organizations must carefully evaluate the total cost of ownership (TCO) to avoid unforeseen expenses. Subscription-based pricing models can become expensive over time, particularly for large organizations with extensive security needs. Conducting regular cost-benefit analyses ensures that the value delivered by SECaaS aligns with the organization's financial constraints and operational goals. This can be managed by:
   - Analysing Usage Patterns: Monitoring network traffic and resource utilization helps optimize subscription tiers.
   - Avoiding Over-Provisioning: Admins should ensure that security measures are appropriately scaled to actual needs, avoiding unnecessary expenses.
   - Using Cost-Effective Tools: Open-source and community-driven tools can complement SECaaS offerings, reducing dependency on paid services.
9) *Security Risks of Outsourcing*: Outsourcing security to a third-party SECaaS provider introduces risks related to trust and control. Organizations must rely on providers to protect sensitive data and systems, yet this lack of direct oversight can create vulnerabilities. Wang & Shen (2013) worn that organizations should implement strong access controls and regularly audit provider performance to mitigate these risks by:
   - Implementing Secure Access Protocols: Technologies such as VPNs (Virtual Private Networks) and SD-WAN (Software-Defined Wide Area Networks) ensure secure communication between organizational networks and SECaaS platforms.

- Monitoring Provider Performance: Engineers should deploy tools to monitor service quality, latency, and security incidents, ensuring that the provider meets agreed-upon standards.
- Establishing Redundancy: Backup security systems or multi-provider strategies can mitigate risks associated with reliance on a single SECaaS provider.
- Regular audits and penetration tests should also be conducted to validate the effectiveness of the provider's security measures

5. Integration of SECaaS with Existing IT Environments

The successful adoption of SECaaS depends not only on its capabilities but also on how effectively it integrates with an organization's existing IT infrastructure. A seamless integration ensures that SECaaS solutions enhance security without disrupting operations, creating redundancies, or compromising performance (Ahn et al., 2024). However, integrating SECaaS into existing IT environments, especially in hybrid or multi-cloud setups, presents unique challenges and requires strategic planning.

One of the primary considerations for integration is compatibility with legacy systems. Many organizations rely on legacy systems that may not inherently support modern cloud-based security services. This can lead to gaps in coverage or require significant effort to bridge the compatibility divide.

Integration also requires careful consideration of organizational workflows and collaboration between in-house IT teams and SECaaS providers. Effective communication and role description are essential to ensure that responsibilities, such as incident response and compliance monitoring, are clearly defined and executed without conflicts. Organizations must establish robust governance frameworks that outline how SECaaS solutions align with their security policies, escalation protocols, and compliance requirements.

Security integration should also focus on minimizing downtime and disruptions during the transition to SECaaS. Phased rollouts, thorough testing, and pilot deployments are recommended strategies to identify and resolve potential issues before full-scale implementation. These steps ensure that the organization can continue its operations without interruptions while gradually adapting to the new security framework.

Finally, the integration of SECaaS into existing IT environments must address potential risks, such as data sovereignty concerns and vendor lock-in. Organizations should prioritize SECaaS providers that offer flexibility and transparency, allowing them to retain control over critical security functions and data. Regular audits and performance reviews are also necessary to evaluate the effectiveness of the integration and ensure that SECaaS solutions meet organizational expectations.

6. Technical Complexities of SECaaS Integration

Integrating SECaaS into existing IT infrastructures is not simply a matter of connecting cloud services through APIs; it involves addressing deep technical challenges that can significantly affect security, performance, and reliability. One of the most pressing issues is protocol translation. Many legacy systems rely on outdated communication standards (e.g., SNMPv2, SOAP-based services, or proprietary protocols), while SECaaS solutions typically operate using modern protocols such as REST, gRPC, or JSON-based APIs. Bridging these differences often requires gateways or middleware capable of translating between protocols in real time. Such translation layers, however, can introduce latency and new attack surfaces if not properly hardened.

Another challenge lies in data format inconsistencies. Legacy systems may generate logs or events in non-standardized formats, whereas SECaaS solutions often expect structured input such as JSON, XML, or formats compliant with standards like Common Event Format (CEF). Inconsistencies can disrupt automated threat detection pipelines and reduce the accuracy of SIEM correlations. Engineering teams must therefore implement normalization tools or adopt log-parsing frameworks to ensure compatibility across heterogeneous systems.

Identity federation adds further complexity. Integrating SECaaS with existing identity and access management frameworks often requires supporting multiple protocols such as SAML, OAuth 2.0, and OpenID Connect simultaneously. Misconfiguration in federation layers can lead to privilege escalation or authentication bypass vulnerabilities, underscoring the need for careful protocol mapping and rigorous testing.

Hybrid and multi-cloud environments also exacerbate these challenges by introducing latency, routing, and encryption overheads. For example, secure tunnelling of traffic between on-premises systems and SECaaS providers may require complex VPN or SD-WAN configurations, which must balance security with performance. Insufficient planning can result in bottlenecks or inconsistent policy enforcement across platforms.

To address these integration difficulties, organizations should adopt modular integration frameworks that rely on open standards, robust middleware, and thorough validation mechanisms. Automated testing environments, including sandboxed deployments, can identify protocol mismatches or format errors before they affect production systems. By confronting these engineering challenges directly, organizations can reduce risks associated with SECaaS integration and ensure that the benefits of scalability and advanced security features are not undermined by technical incompatibilities. Table 3 is a summary of the key insights and potential strategies of different integration aspects.

Table III. Summary of SECaaS integration strategies with existing IT environments

Integration Challenge	**Description**	**Technical Complexities**	**Mitigation Strategies**
Legacy System Compatibility	Older systems may not natively support cloud-based security services.	Proprietary protocols (e.g., SNMPv2, SOAP), limited API support.	Use middleware/gateways, upgrade critical systems, phased migration to standards-compliant tools.
Interoperability in Hybrid/Multi-Cloud	Ensuring consistent security across diverse platforms and vendors.	Inconsistent security policies, latency due to routing across clouds.	Standardize policies, adopt SD-WAN for optimized routing, deploy cloud integration tools with API orchestration.
Protocol Translation	Bridging different communication standards between legacy and modern SECaaS tools.	REST/gRPC vs. legacy SOAP or proprietary formats, real-time translation overhead.	Protocol adapters, secure gateways, sandbox testing for latency/security evaluation.
Data Format Inconsistencies	Logs/events generated in heterogeneous formats incompatible with SECaaS analytics.	Legacy logs vs. structured JSON/XML/CEF formats.	Log normalization tools, parsing frameworks, standard data exchange formats (e.g., CEF, Syslog).
Identity Federation	Integrating IAM across multiple providers and legacy directories.	Supporting SAML, OAuth 2.0, OpenID Connect	Careful protocol mapping, multi-protocol IAM solutions, regular penetration testing.

		simultaneously; misconfiguration risks.	
SIEM Integration	Feeding SECaaS insights into centralized monitoring platforms.	Different log formats, inconsistent threat event structures, data duplication.	API-based integration, normalization, real-time stream processors (e.g., Kafka).
Service Reliability & Performance	Ensuring that added SECaaS layers do not cause downtime or slow systems.	Latency in traffic inspection (e.g., IDPS over VPN tunnels), throughput bottlenecks.	Phased rollout, redundancy in providers, edge-based traffic inspection.
Governance & Compliance	Aligning integration with regulatory and organizational security requirements.	Overlapping regulations (GDPR, PDPA, HIPAA), fragmented compliance audits.	Geo-fencing, audit trails, third-party certifications, compliance-by-design frameworks.

6. Ethical and Trust Issues in Outsourcing Security

While Security-as-a-Service (SECaaS) offers significant technical and operational benefits, it also raises important ethical and trust-related challenges that organizations must carefully consider (Gupta et al., 2025). Unlike traditional in-house security models, outsourcing security responsibilities to external providers involves a transfer of sensitive data, operational visibility, and even partial control over critical systems. This shift creates a dependency that is not only technical but also ethical in nature.

One of the primary concerns is data sovereignty, which refers to the legal and geographical constraints on where data is stored and processed (Pampus & Heisel, 2025). When security services are outsourced, data may cross national boundaries and fall under different regulatory regimes, raising questions about compliance, ownership, and accountability. This is particularly problematic for organizations operating in highly regulated industries, where unauthorized cross-border data flows could lead to legal liabilities and reputational risks.

Another ethical issue lies in the potential misuse of sensitive information. SECaaS providers typically collect and analyse large volumes of logs, user activity data, and system events to detect threats. While this is necessary for effective monitoring, it can also expose organizations to risks of surveillance, profiling, or unauthorized sharing of data with third parties. Without strict contractual and regulatory safeguards, customers must rely heavily on the provider's integrity and governance structures.

To address these issues, organizations should evaluate providers not only on their technical capabilities but also on their ethical posture and trustworthiness. Mechanisms such as transparency reports, independent third-party audits, and well-defined Service Level Agreements (SLAs) can help establish accountability and build confidence (Mushtaque Temrekar, 2025). Transparency reports provide visibility into how data is handled and under what circumstances it may be shared with external entities. Third-party audits verify compliance with industry standards and best practices, while SLAs formalize the responsibilities and obligations of both parties in maintaining data security and privacy.

To better understand the ethical and trust implications of outsourcing security, it is important to examine the role of international standards and frameworks that guide providers and organizations. These standards not only establish technical requirements but also embed principles of accountability, transparency, and data protection, which are critical in fostering trust between SECaaS vendors and clients. While some standards, such as ISO/IEC 27001, focus primarily on information security management, others like GDPR and ISO/IEC 27701 emphasize data privacy and sovereignty. Cloud-specific frameworks, including CSA STAR and ISO/IEC 19086, further address trust by providing mechanisms for assurance, auditability, and contractual clarity. Table 4 provides a comparative analysis of these standards, highlighting their relevance to ethical and trust concerns in SECaaS adoption.

Table IV: Comparative Analysis of Ethical and Trust-Related Standards in SECaaS

Standard/ Framework	Scope & Focus	Ethical/Trust Implications	Relevance to SECaaS
ISO/IEC 27001	Information Security Management Systems (ISMS)	Promotes accountability and continuous risk management	Provides baseline for SECaaS providers to demonstrate secure operations
ISO/IEC 27701	Privacy Information Management Systems (PIMS)	Embeds privacy principles into ISMS, ensuring transparent data handling	Strengthens privacy assurance in SECaaS offerings
CSA STAR	Cloud-specific assurance and certification	Focuses on transparency and provider accountability	Helps clients evaluate SECaaS trustworthiness
ISO/IEC 19086	Cloud Service Level Agreements (SLA)	Emphasizes contractual trust and service transparency	Ensures SECaaS providers meet agreed-upon security levels
GDPR (EU)	Comprehensive data protection and privacy law	Strong emphasis on consent, accountability, and cross-border trust	Forces SECaaS providers handling EU data to align with privacy-by-design
PDPA (Singapore)	Data protection law emphasizing consent, purpose limitation, and accountability	Balances business needs with ethical handling of personal data	Relevant for SECaaS providers in APAC, ensuring compliance and trust-building in cross-border services
CCPA/CPRA (California, US)	Consumer privacy and rights, including data access and deletion	Empowers consumers, strengthens trust via transparency and choice	Affects SECaaS providers handling California residents' data, requiring opt-out mechanisms and disclosure policies

While global privacy regulations such as GDPR, PDPA, and CCPA provide robust frameworks for data protection, their enforcement in practice remains a significant challenge, particularly in the context of cloud computing and Security-as-a-Service (SECaaS). One key difficulty lies in cross-border compliance, as cloud services often involve data transfer across multiple jurisdictions with differing privacy expectations and regulatory mechanisms. This raises complex questions about which laws apply and how they can be enforced consistently against multinational providers.

Another challenge is the limited enforcement capacity in emerging economies, where regulatory authorities may lack the technical expertise, resources, or political support necessary to pursue large-scale violations by powerful cloud vendors. Even in more mature jurisdictions, the scale and complexity of multinational SECaaS operations often make oversight and accountability difficult to sustain.

Real-world cases illustrate both the successes and limitations of current enforcement. For example, the European Union's GDPR enforcement against Meta resulted in billion-euro fines, highlighting regulators' willingness to pursue high-profile violations but also raising debates about proportionality and compliance feasibility (Ruohonen & Hjerppe, 2022). Similarly, Singapore's PDPA enforcement has penalized local and regional firms for inadequate data protection (Greenleaf, 2012), yet the scope and financial weight of sanctions remain far more modest compared to the EU. In the United States, lawsuits under the CCPA demonstrate growing awareness of consumer rights, but fragmented enforcement at the state level creates inconsistencies in outcomes (Huang, 2025).

These cases reveal persistent gaps in enforcement. Disparities between regions create unequal burdens for global SECaaS adoption, while resource limitations hinder smaller regulators from monitoring complex cloud environments effectively. Moreover, enforcement frameworks often struggle to adapt to cloud-specific risks, such as multi-tenancy, vendor lock-in, and shared responsibility models, which traditional legal structures were not designed to address. To achieve meaningful protection, regulatory bodies must collaborate internationally, build stronger technical capacity, and update enforcement mechanisms to reflect the realities of cloud and SECaaS ecosystems.

7. The Future of SECaaS in Cloud Computing

As cloud computing continues to transform how organizations operate, SECaaS is expected to play an increasingly critical role in safeguarding digital ecosystems. With the rapid evolution of technology, threats, and business needs, SECaaS solutions are set to become more advanced, adaptive, and integral to modern IT strategies. This section explores the emerging trends, technological advancements, and future prospects of SECaaS in the ever-changing landscape of cloud computing.

A) Emerging Trends in SECaaS

1. Adoption of Artificial Intelligence and Machine Learning: AI and ML are revolutionizing cybersecurity by enabling SECaaS providers to detect, analyse, and respond to threats with unprecedented speed and accuracy (Kotilainen et al., 2025). These technologies allow for predictive threat detection, where algorithms identify potential risks based on behavioural patterns and historical data.
2. Zero Trust Security Models: The adoption of Zero Trust architectures is reshaping how organizations approach security in cloud environments. Zero Trust emphasizes verifying every user and device, regardless of location or access level. SECaaS providers are increasingly integrating Zero Trust principles into their offerings, providing granular access controls, continuous verification, and micro-segmentation to limit the lateral movement of threats within cloud networks.
3. Integration with IoT and Edge Computing: The increase of Internet of Things (IoT) devices and the rise of edge computing are creating new security challenges (Pawlicki et al., 2023). SECaaS solutions are evolving to address these complexities by extending their capabilities to protect distributed networks, including IoT ecosystems. Advanced SECaaS platforms can monitor and secure data flows across edge devices, ensuring consistent protection in decentralized environments.

B) Technological Advancements Driving SECaaS Evolution

1. Blockchain for Enhanced Security and Transparency: Blockchain technology is being explored as a way to enhance SECaaS solutions by providing immutable audit trails and secure data exchanges. By using blockchain, SECaaS providers can offer transparent and tamper-proof security logs, improving accountability and trust in multi-cloud and hybrid environments (Sarveshwaran et al., 2024).
2. Security Automation and Orchestration: Automation is becoming a cornerstone of SECaaS, enabling faster and more efficient responses to cyber threats. Automated

workflows and security orchestration tools allow organizations to reduce response times, minimize manual intervention, and streamline compliance processes. Future SECaaS offerings are expected to feature more sophisticated automation capabilities, driven by AI and ML.

3. Integration with Advanced Analytics and Big Data: The use of big data analytics in SECaaS is on the rise, providing deeper insights into threat landscapes and enabling more effective security strategies. By analysing vast datasets in real time, SECaaS platforms can uncover hidden patterns, correlations, and vulnerabilities, offering organizations actionable intelligence to strengthen their defences (Zhao et al., 2014).

C) Market Trends and Adoption Drivers

1. Increased Demand for Hybrid and Multi-Cloud Security: As more organizations adopt hybrid and multi-cloud strategies, the demand for SECaaS solutions that can seamlessly operate across different environments is expected to grow. SECaaS providers are developing tools that ensure consistent security policies, regardless of the underlying cloud platforms.
2. Focus on Regulatory Compliance: The complexity of global regulatory requirements continues to drive the need for SECaaS solutions that simplify compliance management. Future offerings are likely to incorporate more advanced compliance automation tools, helping organizations navigate evolving legal landscapes with ease.
3. SME Adoption of SECaaS: Small and medium-sized enterprises (SMEs), traditionally constrained by limited resources, are increasingly adopting SECaaS due to its cost-efficiency and accessibility. This trend is expected to accelerate as SECaaS solutions become more tailored to the needs of smaller organizations.

D) Challenges and Opportunities

While the future of SECaaS is promising, challenges such as data privacy concerns, vendor lock-in risks, and the increasing sophistication of cyber threats remain significant. However, these challenges also present opportunities for innovation. For example, the demand for greater data sovereignty has prompted SECaaS providers to explore localized solutions and hybrid security models that give organizations more control over their data.

1. Convergence of Cybersecurity and Cloud Management: SECaaS platforms are expected to evolve into comprehensive security and cloud management suites, offering unified tools for monitoring, securing, and optimizing cloud environments.
2. Hyper-Personalized Security Solutions: Advances in AI will enable SECaaS providers to deliver hyper-personalized security strategies tailored to the unique risk profiles of individual organizations, providing more effective protection.
3. Expansion into New Frontiers: As technologies like quantum computing emerge, SECaaS will adapt to address new types of threats and opportunities. For example, quantum-safe encryption may become a standard feature in future SECaaS offerings.

E) Sociotechnical Challenges in Adopting SECaaS

While SECaaS offers clear technical and financial advantages, its successful adoption depends heavily on addressing the organizational and human dimensions of change. One of the most significant barriers is internal resistance to outsourcing critical security functions. Many IT teams and decision-makers remain cautious about relying on third-party providers, fearing loss of control, reduced visibility, and potential accountability issues in the event of a breach. This cultural resistance is often stronger in organizations that have traditionally invested in on-premises security infrastructures.

Another important factor is the training and upskilling of existing IT staff. Transitioning to SECaaS requires IT and security teams to shift their roles from directly managing infrastructure to overseeing vendor relationships, monitoring service-level agreements (SLAs), and integrating cloud-based security tools into daily workflows. Without proper training, staff may lack the competencies to evaluate, configure, and optimize SECaaS solutions, leading to both operational inefficiencies and heightened risk exposure.

To overcome these sociotechnical challenges, organizations can benefit from adopting change management practices. This includes engaging stakeholders early in the decision-making process, conducting awareness sessions that emphasize the benefits of SECaaS, and gradually introducing hybrid models to allow teams to adapt without sudden disruption. Furthermore, leadership must clearly articulate the rationale behind the transition, aligning it with broader business goals such as agility, scalability, and compliance.

8. Conclusion

Security-as-a-Service (SECaaS) has fundamentally changed how organizations protect their cloud-based infrastructures, providing a scalable, cost-effective, and adaptive security framework. By using specialized external expertise, enterprises can rapidly deploy advanced defensive measures—vulnerability scanning, intrusion prevention, endpoint protection—without incurring the significant upfront investments typical of traditional, on-premises models. At the same time, SECaaS solutions seamlessly integrate with existing IT environments, support hybrid and multi-cloud strategies, and use evolving technologies such as AI, blockchain, and zero trust.

At the same time, adoption is not without challenges. Beyond technical integration, SECaaS introduces ethical and trust considerations, including data sovereignty, provider accountability, and transparency in managing sensitive information. Comparative analyses show differing adoption patterns between SMEs and large enterprises, where issues such as cost–benefit trade-offs and vendor lock-in require careful strategic planning. Regulatory compliance further complicates adoption, as organizations must navigate different legal regimes such as GDPR, PDPA, HIPAA, ISO 27001, NIST, and CCPA, while also recognizing the enforcement gaps and resource disparities evident in real-world cases.

From a technological standpoint, machine learning has enhanced intrusion detection and prevention systems within SECaaS, but trade-offs remain between accuracy, computational cost, and susceptibility to adversarial threats. Scalability across multi-cloud environments and real-time deployment limitations remain pressing research challenges. Just as critically, organizational and human factors shape the success of SECaaS adoption. Resistance to change, the need for retraining IT staff, and cultural transitions from an on-premises mindset to outsourced security demand slow change management strategies and effective stakeholder communication.

Looking ahead, continuous innovation in AI-driven analytics, automated orchestration, and predictive intelligence will strengthen SECaaS capabilities, while governance frameworks, ethical trust models, and cross-border compliance mechanisms will determine its credibility and sustainability. As businesses expand their reliance on cloud and edge infrastructures, SECaaS must evolve to address emerging needs such as securing IoT ecosystems, supporting regulatory harmonization, and managing sociotechnical change. With robust integration, vigilant governance, and a balanced focus on technology, ethics, and people, SECaaS stands poised to become a cornerstone of cloud security in the digital era..

References

Ahn, S., Gim, G., Jang, S., & Hwang, J. (2024). *A Study on the Integration of Endpoint Security Service Operations Management: Focusing on Cloud Services* (pp. 27–40). https://doi.org/10.1007/978-3-031-53385-3_3

Aljuaid, W. H., & Alshamrani, S. S. (2024). A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. *Applied Sciences*, *14*(13), 5381. https://doi.org/10.3390/app14135381

Asghari, A., & Sohrabi, M. K. (2024). Server placement in mobile cloud computing: A comprehensive survey for edge computing, fog computing and cloudlet. *Computer Science Review*, *51*, 100616. https://doi.org/10.1016/j.cosrev.2023.100616

Ashraf, M. A., Jamal, H., Khan, S. A., Ahmed, Z., & Baig, M. I. (2016). A Heterogeneous Service-Oriented Deep Packet Inspection and Analysis Framework for Traffic-Aware Network Management and Security Systems. *IEEE Access*, *4*, 5918–5936. https://doi.org/10.1109/ACCESS.2016.2609398

Awotunde, J. B., Ayo, F. E., Panigrahi, R., Garg, A., Bhoi, A. K., & Barsocchi, P. (2023). A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. *International Journal of Computational Intelligence Systems*, *16*(1), 31. https://doi.org/10.1007/s44196-023-00205-w

Casola, V., De Benedictis, A., Rak, M., & Villano, U. (2018). Monitoring Data Security in the Cloud: A Security SLA-Based Approach. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (pp. 235–259). Elsevier. https://doi.org/10.1016/B978-0-12-811373-8.00011-2

Chaisiri, S., Ko, R. K. L., & Niyato, D. (2015). A Joint Optimization Approach to Security-as-a-Service Allocation and Cyber Insurance Management. *2015 IEEE Trustcom/BigDataSE/ISPA*, 426–433. https://doi.org/10.1109/Trustcom.2015.403

Conrad, E., Misenar, S., & Feldman, J. (2023). Domain 4: Communication and Network Security. In *CISSP® Study Guide* (pp. 225–293). Elsevier. https://doi.org/10.1016/B978-0-443-18734-6.00003-9

Elsayed, M., & Zulkernine, M. (2019). Offering security diagnosis as a service for cloud SaaS applications. *Journal of Information Security and Applications*, *44*, 32–48. https://doi.org/10.1016/j.jisa.2018.11.006

Farnaaz, N., & Jabbar, M. A. (2016). Random Forest Modeling for Network Intrusion Detection System. *Procedia Computer Science*, *89*, 213–217. https://doi.org/10.1016/j.procs.2016.06.047

Fedele, G., D'Alfonso, L., & Chen, B. (2025). A matching problem between two decoupled multi-agent systems with reference tracking capabilities. *Automatica*, *173*, 112047. https://doi.org/10.1016/j.automatica.2024.112047

Fehis, S., Nouali, O., & Kechadi, T. (2021). Secure encryption key management as a SecaaS based on Chinese wall security policy. *Journal of Information Security and Applications*, *63*, 102975. https://doi.org/10.1016/j.jisa.2021.102975

García-Teodoro, P., Camacho, J., Maciá-Fernández, G., Gómez-Hernández, J. A., & López-Marín, V. J. (2022). A novel zero-trust network access control scheme based on the security profile of devices and users. *Computer Networks*, *212*, 109068. https://doi.org/10.1016/j.comnet.2022.109068

Genge, B., Graur, F., & Enăchescu, C. (2015). Non-intrusive Techniques for Vulnerability Assessment of Services in Distributed Systems. *Procedia Technology*, *19*, 12–19. https://doi.org/10.1016/j.protcy.2015.02.003

Greenleaf, G. (2012). *Singapore's New Data Protection Authority: Strong Enforcement Powers and Business Risks* .

Gupta, P., Sehgal, N. K., & Acken, J. M. (2025). *Trust and Security in a Cloud Environment* (pp. 229–246). https://doi.org/10.1007/978-3-031-59170-9_6

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

Hnamte, V., & Hussain, J. (2023). DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System. *Telematics and Informatics Reports*, *10*, 100053. https://doi.org/10.1016/j.teler.2023.100053

Huang, M.-L. (2025). Digital Privacy in the Age of Surveillance: A Comparative Study of GDPR and CCPA. *OTS Canadian Journal*, *4*(7), 65–74. https://doi.org/10.58840/1t99rb13

Jafari, N., Alsadoon, A., Withana, C. P., Beg, A., & Elchouemi, A. (2016). Designing a Comprehensive Security Framework for Smartphones and Mobile Devices. *American Journal of Engineering and Applied Sciences*, *9*(3), 724–734. https://doi.org/10.3844/ajeassp.2016.724.734

Jayshree, J., & Leena, R. (2013). Intrusion Detection System using Support Vector Machine. *International Journal of Applied Information Systems (IJAIS)*.

Jurgała, P., Kurek, T., & Niemiec, M. (2022). Preserving Privacy of Security Services in the SecaaS Model. *Information & Security: An International Journal*, *53*, 47–64. https://doi.org/10.11610/isij.5304

Kaluvuri, S. P., Egner, A. I., den Hartog, J., & Zannone, N. (2015). SAFAX â€" An Extensible Authorization Service for Cloud Environments. *Frontiers in ICT*, *2*. https://doi.org/10.3389/fict.2015.00009

Khan, A. R., Kashif, M., Jhaveri, R. H., Raut, R., Saba, T., & Bahaj, S. A. (2022). Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions. *Security and Communication Networks*, *2022*, 1–13. https://doi.org/10.1155/2022/4016073

Kotilainen, P., Mäkitalo, N., Systä, K., Mehraj, A., Waseem, M., Mikkonen, T., & Murillo, J. M. (2025). Allocating distributed AI/ML applications to cloud-edge continuum based on privacy, regulatory, and ethical constraints. *Journal of Systems and Software*, 112333. https://doi.org/10.1016/j.jss.2025.112333

Lakshminarayana, S. K., & Basarkod, P. I. (2023). Unification of K-Nearest Neighbor (KNN) with Distance Aware Algorithm for Intrusion Detection in Evolving Networks Like IoT. *Wireless Personal Communications*, *132*(3), 2255–2281. https://doi.org/10.1007/s11277-023-10722-8

Mostafa, A. M., Rushdy, E., Medhat, R., & Hanafy, A. (2023). An identity management scheme for cloud computing: Review, challenges, and future directions. *Journal of Intelligent & Fuzzy Systems*, *45*(6), 11295–11317. https://doi.org/10.3233/JIFS-231911

Mukherjee, S., & Sharma, N. (2012). Intrusion Detection using Naive Bayes Classifier with Feature Reduction. *Procedia Technology*, *4*, 119–128. https://doi.org/10.1016/j.protcy.2012.05.017

Muneer, S., Farooq, U., Athar, A., Ahsan Raza, M., Ghazal, T. M., & Sakib, S. (2024). A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis. *Journal of Engineering*, *2024*(1). https://doi.org/10.1155/2024/3909173

Mushtaque Temrekar, Ms. M. (2025). A Comparative Analysis of Global Data Privacy Regulations and Their Implementation by Major Cloud Service Providers. *INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, *09*(05), 1–9. https://doi.org/10.55041/IJSREM46907

Nikhitha, M., & Jabbar, Dr. M. A. (2019). K Nearest Neighbor Based Model for Intrusion Detection System. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2), 2258–2262. https://doi.org/10.35940/ijrte.B2458.078219

Pampus, J., & Heisel, M. (2025). A Delimitation of Data Sovereignty From Privacy. In *Empowering Digital Sovereignty* (pp. 1–24). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9137-2.ch001

Pawlicki, M., Pawlicka, A., Kozik, R., & Choraś, M. (2023). The survey and meta-analysis of the attacks, transgressions, countermeasures and security aspects common to the Cloud, Edge and IoT. *Neurocomputing*, *551*, 126533. https://doi.org/10.1016/j.neucom.2023.126533

R. Tahri, A. Lasbahani, A. Jarrar, & Y. Balouki. (2024). Intelligent Intrusion Detection Using Decision Trees and the NSL-KDD Dataset: An All-Inclusive Method for Cyber Attack Detection. *Journal of Southwest Jiaotong University*, *59*(5). https://doi.org/10.35741/issn.0258-2724.59.5.13

Ranaweera, P., Imrith, V. N., Liyanag, M., & Jurcut, A. D. (2020). Security as a Service Platform Leveraging Multi-Access Edge Computing Infrastructure Provisions. *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC40277.2020.9148660

Rullo, A., Midi, D., Mudjerikar, A., & Bertino, E. (2024). Kalis2.0—A SECaaS-Based Context-Aware Self-Adaptive Intrusion Detection System for IoT. *IEEE Internet of Things Journal*, *11*(7), 12579–12601. https://doi.org/10.1109/JIOT.2023.3333948

Ruohonen, J., & Hjerppe, K. (2022). The GDPR enforcement fines at glance. *Information Systems*, *106*, 101876. https://doi.org/10.1016/j.is.2021.101876

Sarveshwaran, V., Pandiaraj, S., Bindu, G., Ganesan, V., & Swamidason, I. T. J. (2024). Binarized Spiking Neural Network with blockchain based intrusion detection framework for enhancing privacy and security in cloud computing environment. *Applied Soft Computing*, *154*, 111218. https://doi.org/10.1016/j.asoc.2023.111218

Settanni, F., Regano, L., Basile, C., & Lioy, A. (2023a). A Model for Automated Cybersecurity Threat Remediation and Sharing. *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, 492–497. https://doi.org/10.1109/NetSoft57336.2023.10175486

Settanni, F., Regano, L., Basile, C., & Lioy, A. (2023b). A Model for Automated Cybersecurity Threat Remediation and Sharing. *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, 492–497. https://doi.org/10.1109/NetSoft57336.2023.10175486

Sharma, D. H., Dhote, C. A., & Potey, M. M. (2016). Implementing Intrusion Management as Security-as-a-service from cloud. *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, 363–366. https://doi.org/10.1109/CSITSS.2016.7779387

Shen, Y., Li, Y., Wu, L., Liu, S., & Wen, Q. (2013). *Security Information and Event Management Implementation Guidance* (pp. 94–115). https://doi.org/10.4018/978-1-4666-4801-2.ch005

Shirley C P, Thanga Helina S, Thusita S, & Okesh A. (2025). Machine Learning for Cloud Security: A Systematic Review. *Journal of Information Systems Engineering and Management* , *10*(37), 517–529.

Srinadh, V., Swaminathan, B., & Vidyadhari, Ch. (2023). Blockchain-Integrated Advanced Persistent Threat Detection Using Optimized Deep Learning-Enabled Feature Fusion. *Journal of Uncertain Systems*, *16*(03). https://doi.org/10.1142/S1752890922500179

Stephenson Achankeng. (2025). Analysis of Prevention Techniques against DDoS and SQL Injection Attack in Network and Cloud Environment. *Journal of Cloud Computing*.

Su, L., Bai, W., Zhu, Z., & He, X. (2021). Research on Application of Support Vector Machine in Intrusion Detection. *Journal of Physics: Conference Series*, *2037*(1), 012074. https://doi.org/10.1088/1742-6596/2037/1/012074

Talib, A. M., Atan, R., Abdullah, R., & Murad, M. A. A. (2012). Security Facilitation in Collaborative Cloud Data Storage Implementation Environment Based on Multi Agent System Architecture. *Journal of Software Engineering*, *6*(3), 49–64. https://doi.org/10.3923/jse.2012.49.64

Wang, Y., & Shen, J. (2013). CloudProxy: A NAPT Proxy for Vulnerability Scanners based on Cloud Computing. *Journal of Networks*, *8*(3). https://doi.org/10.4304/jnw.8.3.607-615

Yang, L., Moubayed, A., Hamieh, I., & Shami, A. (2019). Tree-Based Intelligent Intrusion Detection System in Internet of Vehicles. *2019 IEEE Global Communications Conference (GLOBECOM)*, 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013892

Yuan, H., Xia, Y., Zhang, J., Yang, H., & Mahmoud, M. S. (2020). Stackelberg-Game-Based Defense Analysis Against Advanced Persistent Threats on Cloud Control System. *IEEE Transactions on Industrial Informatics*, *16*(3), 1571–1580. https://doi.org/10.1109/TII.2019.2925035

Zhao, J., Wang, L., Tao, J., Chen, J., Sun, W., Ranjan, R., Kołodziej, J., Streit, A., & Georgakopoulos, D. (2014). A security framework in G-Hadoop for big data computing across distributed Cloud data centres. *Journal of Computer and System Sciences*, *80*(5), 994–1007. https://doi.org/10.1016/j.jcss.2014.02.006