International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 9, Issue 4, (December 2023), www.ijtmh.com

Securing Machine-to-Machine Communications in the Age of Non-Human Identities

Author

Oluwatosin Oladayo Aramide

NetApp Ireland Limited. Ireland.

Email: aoluwatosin10@gmail.com

Abstract

The digital age of non-human identities The world of non-human identities is one that is predominated by digital actors that communicate, authenticate and exchange data without human intervention, and this is a result of rapid proliferation of connected devices, autonomous systems and application programming interfaces (APIs). With the Machine-to-Machine (M2M) communications now becoming the basis of operations in such industries as manufacturing, healthcare, transport, and smart cities, the safety of such communications is paramount. But existing identity and access management systems, developed to secure the access of human users, are inadequate in coping with the distinctive difficulties of the highly distributed, highly mobile, and short-lived machine identities.

This document will analyze these threats and others in the M2M communications and outline how the threats are evolving and this should be an eye opener especially to the security industry. It describes the existing technologies and protocols to authenticate and authorize the identities of non-humans, e.g., PKI, OAuth 2.0, and new decentralized identities frameworks and analyzes how these can perform in praxis. We also study the issues of machine identity management life lifecycle, scalability, and modeling of trust in the various heterogeneous environments. Lastly, future research directions coming out of the research area are also proposed upon AI-driven anomaly detection, zero trust architectures, and decentralized identity governance to further consolidate machine-to-machine security foundational structures.

Keywords: M2M-based communications, non-human identities, IoT security, machine identity management, PKI, API security, zero trust architecture, decentralized identity, autonomous systems, cybersecurity.

DOI: 10.21590/ijtmh.2023090408

1. Introduction

The world of digital interoperation is changing radically as a result of unprecedented proliferation of devices and systems able to communicate and interact without any human intervention. With the emergence of such communications, the trend towards Machine-to-Machine (M2M) communications, which means automated communication between machines, including IoT sensors, self-driving cars, industrial robots, APIs, and cloud-native services. Such communications are the core of the modern infrastructure used in smart manufacturing applications, telemedicine, logistics, defense, and urban services.

The crux of this transformation is, therefore, the creation of the non-human identities, digital agents that can have credentials, engage in transactions, and socialize over the distributed networks. In contrast to the traditional user identities, which are associated with individuals, and the laws of which people know at least, the non-human identities are dynamic, and they may or may not have a long life, but they can be scaled massively. Industry data shows that in enterprise networks, machine identities now exceed human identities 45:1, and it is time to reconsider the security architecture in the era of non-humans.

Such efficiency and automation of M2M communication come at the price of a huge increase in the attack surface, and this is a fact that traditional cybersecurity plans may often ignore. The non-human entities may not have consistent identity management, may use default or hard coded credentials, or may send information via an unencrypted communications channel. Among such tactics are the increasing exploits of such gaps by the attackers:

- Miming trusted devices / APIs
- Sessions commandeering Hijacking communications Sessions
- Stealing information through infected machine agents
- Use of machine trust chains to shift into sensitive systems

Even though the reliance on autonomous systems continues to increase, the majority of the available identity and access management (IAM) structures are not well-positioned to manage the volume, variety, and fluidity of machine identities. Other security measures meant to support humans, e.g., multi-factor authentication, role-based access control, and manual key provisioning usually cannot cope with machine workflows that require instant authentication and low latency execution and are unable to scale without distributed trust.

Additionally, the problem is worsened by the fact that there are no common forms of governance of machine identities, particularly in contexts where individuals have many clouds, edge devices, and legacy systems. The fact that M2M communications are increasingly becoming a critical part of the infrastructure and national security, it no longer behooves enough to ensure the security of these interactions is just a technological concern, but a strategic one as well.

This study proposes to discuss the security consequences of the non-human identity explosion in the M2M environments. It investigates:

- The changing phenomenon of non-human identities
- The threats that are applied against M2M interactions
- Solutions to machine identity management today and in the future

The important problems with the scalability, key lifecycle management and enforcement of trust are all considered.

Finally, the paper aims at contributing to the discussion on how cybersecurity frameworks should be modified to accommodate a world in which machines are not only parts of the network; they become the main players.

2. Understanding Non-Human Identities

In the rapidly evolving digital landscape, the concept of **identity** is no longer limited to human users. Non-human identities such as IoT devices, APIs, microservices, bots, autonomous agents, and virtual machines now dominate machine-to-machine (M2M) communication ecosystems. These entities require secure, persistent, and verifiable digital identities to interact autonomously within and across organizational boundaries. As the number of such entities surpasses the number of human users in enterprise networks, a shift in identity management frameworks is necessary.

2.1. Definition and Characteristics of Non-Human Identities

A non-human identity refers to a unique, verifiable digital persona assigned to a machine or software component that participates in networked systems. Unlike human identities, which rely on biometric, password-based, or behavioral authentication, non-human identities use cryptographic keys, certificates, tokens, or device fingerprints.

Key characteristics include:

- **Autonomy**: Operates without direct human interaction.
- **Ephemerality**: May exist temporarily (e.g., containers, microservices).
- **Scalability**: Tens of thousands of identities can be generated dynamically.
- **Interoperability**: Interacts across diverse platforms and protocols.

2.2. Types of Non-Human Identities

Non-human identities can be categorized based on function and lifecycle. The most common include:

- **IoT Devices**: Embedded sensors, wearables, smart appliances, and industrial machinery.
- **APIs**: Interfaces used to enable system-to-system interaction (e.g., financial data sharing).
- **Bots and RPA Agents**: Software robots performing tasks traditionally done by humans.
- **Cloud Workloads**: Containers, virtual machines (VMs), and serverless functions.
- **Edge Devices**: Devices operating at the edge of networks, often in remote or resource-constrained environments.
- **Autonomous Agents**: AI-powered systems that make decisions independently.

2.3. Identity Lifecycle of Machines

Just like human users, non-human entities follow a lifecycle that needs to be secured and governed. The major stages include:

1. **Provisioning** – Initial creation and configuration of the machine identity using credentials or certificates (e.g., X.509).
2. **Authentication & Authorization** – Granting access to resources via identity-based policies (e.g., role-based access).
3. **Monitoring & Renewal** – Continuous validation of credentials, certificate rotation, and behavioral monitoring.
4. **Decommissioning** – Revocation and secure disposal of identity credentials when the entity is no longer active.

Failure to manage this lifecycle effectively can lead to orphaned identities and security blind spots often exploited in lateral movement and impersonation attacks.

2.4. Comparison with Human Identity Management

While both human and machine identities aim to control access and establish trust, their management differs fundamentally:

Aspect	Human Identity	Non-Human Identity
Identity Issuance	Often centralized (HR, IT)	Decentralized or automated provisioning
Authentication Method	Passwords, biometrics, MFA	API keys, certificates, tokens
Lifecycle	Relatively static	Highly dynamic and short-lived
Volume & Scale	Limited to number of users	Can exceed millions
Trust Relationships	Hierarchical and organizational	Distributed across systems and vendors
Governance Frameworks	Mature IAM solutions	Emerging machine identity platforms

2.5. Identity Explosion and the Machine Identity Gap

As organizations scale digital operations, the number of machine identities grows exponentially creating a phenomenon known as the "machine identity gap." While human identity management is typically well-resourced and centrally governed, the same rigor is often absent for machines, resulting in:

- Misconfigured or default credentials
- Stale or unmonitored certificates
- Unauthorized access by rogue devices or services

Analysts have noted that most enterprises underestimate the number of active machine identities, and that unmanaged credentials are often a leading cause of security incidents.

2.6. Emerging Solutions and Standards

To address the growing complexity of machine identity, industry and academic research have introduced new solutions:

- Machine Identity Management Platforms (e.g., Venafi, AppViewX) for certificate automation and policy enforcement.
- Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) for machine-to-machine trust in federated systems.
- Zero Trust principles applied to machines, requiring continuous identity verification and context-aware access decisions.

Security standards such as NIST SP 800-207, ISO/IEC 29115, and RFC 8990 provide guidance on secure identity proofing and federation for non-human entities.

Non-human identities are now a critical part of the cybersecurity threat surface. Understanding their diversity, operational roles, and lifecycle is essential for building secure, scalable, and resilient M2M environments. As organizations adopt automation and connected systems, prioritizing machine identity governance is not optional; it is foundational to enterprise security.

3. Threat Landscape in M2M Communications

Machine-to-Machine (M2M) communications underpin a vast array of applications in modern digital infrastructure from industrial IoT systems and autonomous vehicles to healthcare monitoring devices and cloud-native APIs. As the number of non-human identities expands exponentially, so too does the attack surface available to adversaries. Unlike traditional user-centric threats, M2M threats exploit gaps in trust models, authentication protocols, and the identity lifecycle of machines. This section explores the most critical threat vectors that compromise the confidentiality, integrity, and availability of M2M ecosystems.

3.1. Device Impersonation and Spoofing

M2M communications often rely on lightweight or implicit trust assumptions, particularly in resource-constrained environments (e.g., sensor networks, embedded controllers). Attackers exploit this by:

- Cloning device credentials or forging certificates to impersonate trusted devices.
- Spoofing MAC/IP addresses to blend malicious nodes into legitimate network topologies.
- Triggering data manipulation, false telemetry reporting, or command injection.

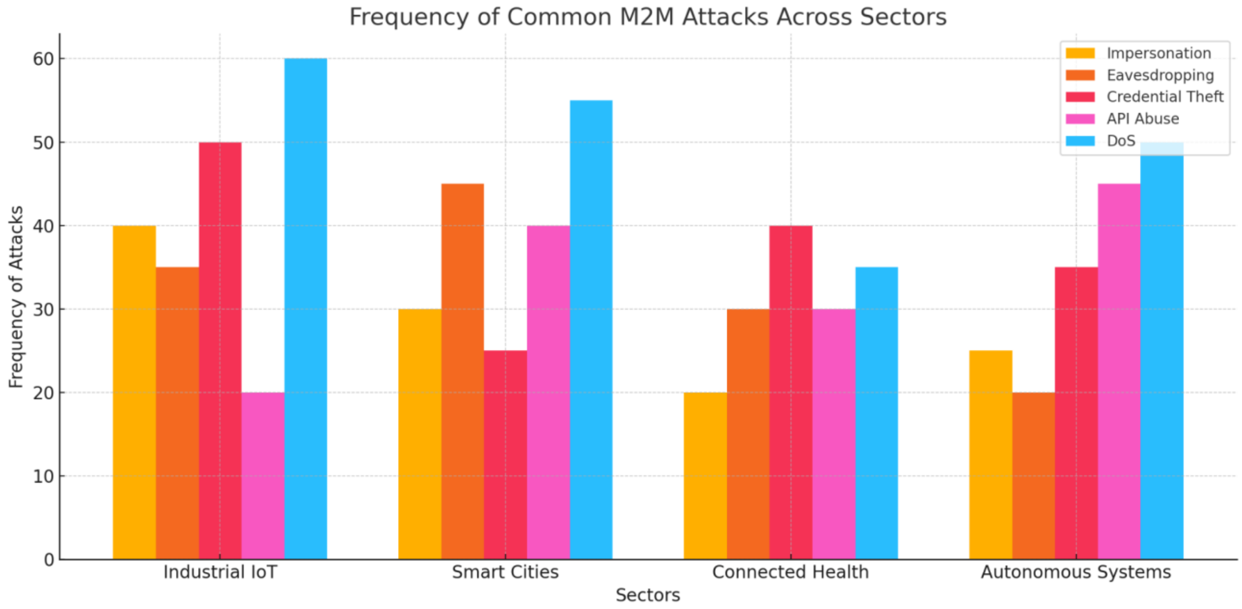
These attacks are especially dangerous in critical systems such as industrial automation, where false commands can result in physical harm or operational downtime.

3.2. Man-in-the-Middle (MitM) and Eavesdropping

A lack of end-to-end encryption or weak transport-layer security makes many M2M channels susceptible to interception. Through MitM attacks, adversaries can:

- Intercept and modify data packets between machines
- Harvest machine credentials or tokens
- Replay commands to mimic valid operations

Such attacks are prevalent in legacy industrial IoT (IIoT) environments and smart home networks, where security protocols are often minimal or outdated.



The bar chart shows the frequency of common M2M attacks across different sectors.

3.3. Credential Theft and Key Compromise

In M2M ecosystems, machines authenticate using certificates, pre-shared keys (PSKs), tokens, or API keys. These credentials are often:

- Stored insecurely (e.g., hard-coded in firmware or exposed in logs)
- Poorly rotated, increasing exposure time if compromised
- Distributed without tracking, especially in cloud-native environments

Compromised credentials can allow unauthorized access to privileged services, escalate privileges, or pivot laterally through the network.

3.4. API Abuse and Unauthorized Access

APIs serve as the primary interface for many machine identities. However, poorly secured APIs can expose backend systems to:

- Data scraping or exfiltration attacks
- Function abuse through excessive or malformed requests (e.g., API fuzzing)
- Privilege escalation, especially if role-based access control (RBAC) is misconfigured

Attackers increasingly target APIs in microservices and containerized environments where machines communicate rapidly and autonomously.

3.5. Denial-of-Service (DoS) and Resource Exhaustion

M2M environments often involve constrained devices with limited CPU, memory, and network bandwidth. Attackers can exploit these limitations through:

- Flooding attacks (e.g., CoAP/UDP floods)
- Battery draining attacks in mobile or edge devices
- Resource starvation that disrupts legitimate machine interactions

Such attacks can cascade through interconnected systems, disrupting service availability or degrading performance in safety-critical applications.

3.6. Supply Chain and Firmware Manipulation

Machines often rely on third-party components, firmware updates, and over-the-air (OTA) provisioning. These supply chain dependencies introduce risks such as:

- Tampered firmware updates containing malicious payloads
- Compromised software libraries injected during development or deployment
- Insecure update channels, lacking integrity verification

Firmware-based attacks are particularly stealthy and persistent, allowing long-term surveillance or sabotage of M2M systems.

3.7. Insider and Rogue Device Risks

Not all M2M threats originate from external attackers. Insider threats can introduce rogue devices or manipulate legitimate machines to:

- **Bypass monitoring systems**
- **Inject malicious configurations or telemetry**
- **Trigger policy violations undetected**

Rogue machines are often difficult to detect in large-scale deployments, especially when devices operate autonomously or intermittently.

The threat landscape in M2M communications is complex and evolving. Machines are often “trusted by default,” operate continuously, and can be deployed at massive scale making them ideal targets for both opportunistic and targeted attacks. As M2M communication becomes more pervasive across sectors, it is critical to evolve from human-centric security paradigms to frameworks that recognize and protect the unique characteristics of non-human identities.

4. Security Frameworks and Protocols for M2M

Securing Machine-to-Machine (M2M) communication is a cornerstone of cyber-physical infrastructure, particularly in environments dominated by non-human identities such as IoT devices, autonomous agents, APIs, and digital twins. Unlike human interactions, which benefit from session-based access control and behavioral monitoring, machine interactions require persistent, automated, and secure protocols that can scale with minimal human intervention. This section explores the primary frameworks, architectures, and protocols used to secure M2M systems, highlighting their applicability, benefits, and limitations.

4.1. Public Key Infrastructure (PKI) for Machines

Public Key Infrastructure remains a foundational component in securing M2M communications, providing authentication, integrity, and encryption through digital certificates and asymmetric cryptography. In M2M contexts:

- Devices are issued X.509 certificates for identity binding.
- Mutual TLS (mTLS) is used to authenticate both endpoints.
- Certificate revocation and renewal must be automated at scale.

However, traditional PKI models were not designed for environments with millions of lightweight, transient devices, making scalability and lifecycle management key challenges.

4.2. Transport Layer Security (TLS) and Datagram TLS (DTLS)

TLS and its counterpart for UDP-based communication, DTLS, are widely adopted for ensuring secure communication channels between machines. These protocols offer:

- End-to-end encryption
- Integrity protection
- Optional client-side authentication

DTLS is especially useful in resource-constrained IoT environments and real-time systems such as industrial sensors. Nevertheless, the computational overhead of TLS/DTLS handshakes and key exchanges can strain low-power devices unless optimized.

4.3. OAuth 2.0 and Device Authorization Flows

OAuth 2.0, originally designed for delegating access between web applications, has been adapted for M2M use cases via Client Credentials Grant and Device Authorization Grant flows. These allow:

- Token-based access control
- Secure service-to-service authorization
- Scoped access to APIs or cloud resources

However, OAuth assumes the presence of a trusted authorization server and may not be suitable for decentralized edge networks where continuous connectivity cannot be guaranteed.

Here is a comparative table showing key M2M (Machine-to-Machine) security protocols:

Protocol	**Communication Type**	**Security Features**	**Device Suitability**	**Scalability**	**Common Use Cases**
mTLS	Client-Server (TCP)	Mutual authentication, data encryption, integrity	Suitable for high-capacity devices	High	Industrial IoT, secure enterprise APIs, cloud services
DTLS	Datagram (UDP)	Encryption, message integrity, replay protection	Suitable for constrained devices	Moderate	Smart grid, sensor networks, constrained environments

OAuth 2.0	Web-based/API	Token-based access control, authorization delegation	Best for cloud-connected applications	High	API access, smart city services, healthcare data sharing
CoAP with DTLS	REST over UDP	Lightweight encryption, replay protection, message integrity	Ideal for low-power constrained devices	Moderate to High	Smart lighting, environmental monitoring, industrial sensors
MQTT with TLS	Publish/Subscribe (TCP)	Data encryption, authentication, integrity	Efficient for low-bandwidth devices	High	Real-time telemetry, asset tracking, home automation

4.4. Lightweight Machine-to-Machine (LwM2M) and CoAP

Designed for constrained environments, LwM2M (Lightweight M2M) builds on CoAP (Constrained Application Protocol) with embedded support for:

- Bootstrapping and registration of devices
- Access control lists (ACLs)
- Secure firmware updates over DTLS

LwM2M is widely used in cellular IoT and embedded systems, especially where energy efficiency and low memory footprint are priorities.

4.5. Identity and Access Management (IAM) for Devices

Device-level IAM involves managing:

- Unique digital identities for each machine
- Role-based and attribute-based access policies
- Lifecycle governance (onboarding, monitoring, decommissioning)

Modern IAM platforms (e.g., AWS IoT Core, Azure IoT Hub) offer integration with cloud-native access controls, but cross-platform and vendor-neutral IAM remains a gap in the current M2M security landscape.

4.6. Decentralized Identifiers (DIDs) and Verifiable Credentials

A growing body of research and pilot implementations has explored the use of Decentralized Identifiers (DIDs) for M2M identity and trust management. DIDs:

- Operate without centralized authorities
- Allow machines to self-assert and verify identity via cryptographic proofs
- Support interoperability across domains

When combined with Verifiable Credentials (VCs), DIDs offer a flexible and privacy-preserving alternative to traditional certificates. However, adoption is still limited due to:

- Lack of performance benchmarks in large-scale networks
- Immature tooling and governance models

4.7. Zero Trust Architecture (ZTA) for M2M

Zero Trust principles "never trust, always verify" are increasingly applied to M2M communications. In ZTA environments:

- Every communication is authenticated and authorized dynamically
- Devices are continuously monitored for behavioral anomalies
- Policy enforcement is context-aware (location, time, usage pattern)

M2M Zero Trust implementation requires the convergence of:

- Strong identity (often through PKI or DIDs)
- Fine-grained access control
- Continuous telemetry and machine behavior analysis

While still in early stages for M2M contexts, ZTA is seen as future-proof against advanced persistent threats (APTs) and lateral movement within machine networks.

Security frameworks for M2M communication are evolving rapidly to keep pace with the explosion of non-human identities. While legacy approaches like TLS and PKI continue to play a central role, new paradigms such as decentralized identity and zero trust architectures are emerging to fill the gaps in scalability, trust, and autonomy. A hybrid model combining lightweight protocols, automated credential management, and adaptive access policies will be essential for securing the next generation of machine-driven systems.

5. Challenges in Securing Non-Human Entities

As machine-to-machine (M2M) communications scale across cloud, edge, and on-premise environments, the emergence of non-human identities including IoT devices, software agents, APIs, bots, and digital twins has introduced a complex array of security challenges. These non-human entities interact continuously, often autonomously, and typically operate without direct human oversight. Their security, therefore, requires mechanisms that go beyond traditional user-centric models.

The following subsections identify and analyze the key challenges associated with securing non-human entities in dynamic M2M ecosystems.

5.1. Identity Provisioning and Lifecycle Management

Unlike human identities, which follow predictable enrollment and authentication workflows, non-human identities are often:

- Created and destroyed dynamically (e.g., containers, serverless functions)
- Scaled horizontally across thousands of instances
- Assigned varying levels of access and privilege based on task

Secure lifecycle management from identity issuance, key generation, renewal, revocation, to decommissioning is difficult at scale. Mismanaged credentials and static secrets are common attack vectors.

5.2. Scalability in Heterogeneous Environments

Modern enterprise systems may include:

- Billions of IoT sensors
- Multiple cloud providers and APIs
- Edge devices and fog nodes
- On-premise legacy systems

Ensuring uniform identity governance and policy enforcement across such a fragmented landscape is a formidable challenge. Differences in device capabilities (e.g., memory, computation), connectivity, and supported protocols complicate standardization efforts.

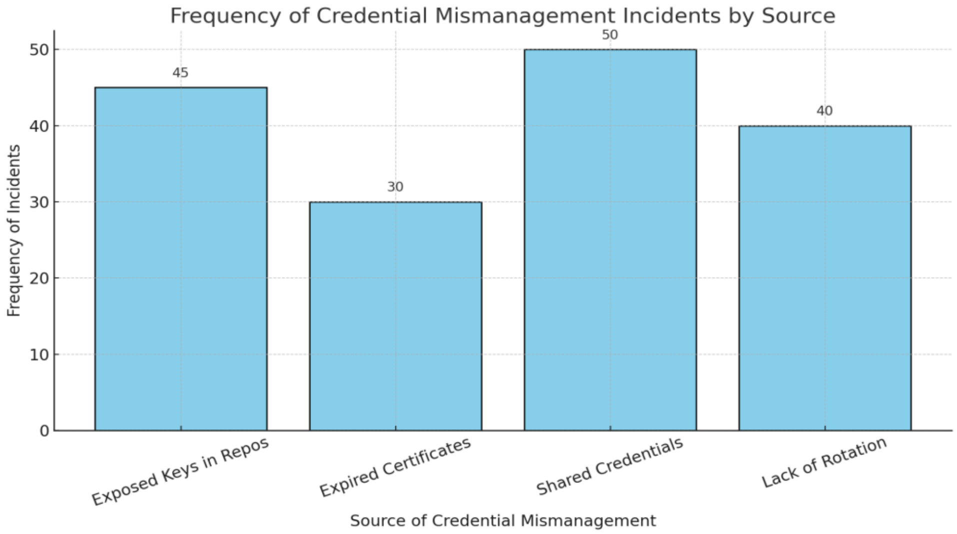
Cloud-native approaches like Zero Trust Architecture (ZTA) and microsegmentation show promise but face practical implementation constraints in constrained or low-power environments.

5.3. Credential Management and Secret Rotation

Many machines still rely on hardcoded credentials, API keys, or certificates that:

- Are manually configured
- Rarely rotated or expire
- Are exposed in code repositories or configuration files

Lack of automated secret rotation or vaulting systems increases the risk of credential theft and lateral movement. Dynamic environments (e.g., Kubernetes) demand short-lived credentials and identity-bound tokens, which are still underutilized.



The bar graph displaying the frequency of credential mismanagement incidents by source.

5.4. Trust Modeling Across Distributed Systems

In M2M ecosystems, machines often need to communicate across organizational and jurisdictional boundaries. Trust establishment in such systems is difficult because:

- There is no global trust authority
- Devices may belong to different trust domains
- Continuous authentication is needed to validate dynamic behavior

While federated identity models and PKI can bridge trust boundaries, trust decay and revocation latency remain problems in real-time systems. Attackers can exploit temporary trust relationships to pivot across environments.

5.5. Lack of Unified Standards and Interoperability

Despite progress in identity standards (e.g., X.509, OAuth 2.0, mTLS, SPIFFE), there is no unified framework for securing non-human identities across vendors, platforms, and ecosystems. This leads to:

- Fragmented implementations
- Vendor lock-in
- Difficulty in auditing and compliance enforcement

Standardization bodies such as NIST, IETF, and the OpenID Foundation have initiated working groups, but adoption remains slow in non-enterprise and industrial environments.

5.6. Limited Visibility and Anomaly Detection

Many machine identities operate "invisibly" within automated systems, generating high volumes of network traffic, log data, and API calls. Security teams often lack:

- Baseline behavior models for machine entities
- Real-time visibility into credential use
- Alerts tuned for machine-only environments

Traditional security information and event management (SIEM) systems are human-centric and may miss subtle anomalies in machine communications.

Behavioral analytics and machine learning approaches offer promise but require clean training data and integration into real-time monitoring workflows.

5.7. Compliance and Policy Enforcement at Scale

Compliance with data protection regulations and internal policies becomes more difficult when dealing with thousands of dynamic, autonomous identities. Key concerns include:

- How to log, audit, and report on non-human entity actions
- Mapping machine activities to regulatory frameworks (e.g., GDPR, HIPAA)
- Defining access policies that remain consistent across cloud, edge, and hybrid environments

Without robust governance frameworks, organizations face increased risk of both security breaches and compliance violations.

Securing non-human entities is not simply an extension of human identity management, it requires a new paradigm that emphasizes automation, distributed trust, and adaptive intelligence. Addressing the challenges outlined in this section will be central to the development of secure and resilient machine-to-machine communication infrastructures. The path forward lies in unifying identity standards, integrating automated credential management, and embedding AI-driven monitoring at scale.

5. Challenges in Securing Non-Human Entities

As machine-to-machine (M2M) communications scale across cloud, edge, and on-premise environments, the emergence of non-human identities including IoT devices, software agents, APIs, bots, and digital twins has introduced a complex array of security challenges. These non-human entities interact continuously, often autonomously, and typically operate without direct human oversight. Their security, therefore, requires mechanisms that go beyond traditional user-centric models.

The following subsections identify and analyze the key challenges associated with securing non-human entities in dynamic M2M ecosystems.

5.1. Identity Provisioning and Lifecycle Management

Unlike human identities, which follow predictable enrollment and authentication workflows, non-human identities are often:

- Created and destroyed dynamically (e.g., containers, serverless functions)
- Scaled horizontally across thousands of instances
- Assigned varying levels of access and privilege based on task

Secure lifecycle management from identity issuance, key generation, renewal, revocation, to decommissioning is difficult at scale. Mismanaged credentials and static secrets are common attack vectors.

5.2. Scalability in Heterogeneous Environments

Modern enterprise systems may include:

- Billions of IoT sensors
- Multiple cloud providers and APIs
- Edge devices and fog nodes
- On-premise legacy systems

Ensuring uniform identity governance and policy enforcement across such a fragmented landscape is a formidable challenge. Differences in device capabilities (e.g., memory, computation), connectivity, and supported protocols complicate standardization efforts.

Cloud-native approaches like Zero Trust Architecture (ZTA) and microsegmentation show promise but face practical implementation constraints in constrained or low-power environments.

5.3. Credential Management and Secret Rotation

Many machines still rely on hardcoded credentials, API keys, or certificates that:

- Are manually configured
- Rarely rotated or expire
- Are exposed in code repositories or configuration files

Lack of automated secret rotation or vaulting systems increases the risk of credential theft and lateral movement. Dynamic environments (e.g., Kubernetes) demand short-lived credentials and identity-bound tokens, which are still underutilized.

5.4. Trust Modeling Across Distributed Systems

In M2M ecosystems, machines often need to communicate across organizational and jurisdictional boundaries. Trust establishment in such systems is difficult because:

- There is no global trust authority
- Devices may belong to different trust domains
- Continuous authentication is needed to validate dynamic behavior

While federated identity models and PKI can bridge trust boundaries, trust decay and revocation latency remain problems in real-time systems. Attackers can exploit temporary trust relationships to pivot across environments.

5.5. Lack of Unified Standards and Interoperability

Despite progress in identity standards (e.g., X.509, OAuth 2.0, mTLS, SPIFFE), there is no unified framework for securing non-human identities across vendors, platforms, and ecosystems. This leads to:

- Fragmented implementations
- Vendor lock-in
- Difficulty in auditing and compliance enforcement

Standardization bodies such as NIST, IETF, and the OpenID Foundation have initiated working groups, but adoption remains slow in non-enterprise and industrial environments.

5.6. Limited Visibility and Anomaly Detection

Many machine identities operate "invisibly" within automated systems, generating high volumes of network traffic, log data, and API calls. Security teams often lack:

- Baseline behavior models for machine entities
- Real-time visibility into credential use
- Alerts tuned for machine-only environments

Traditional security information and event management (SIEM) systems are human-centric and may miss subtle anomalies in machine communications.

Behavioral analytics and machine learning approaches offer promise but require clean training data and integration into real-time monitoring workflows.

The table below shows anomaly detection techniques and their effectiveness in monitoring human vs. non-human traffic:

Technique	Human Traffic Effectiveness	Non-Human Traffic Effectiveness	Notes
Signature-	High (known	Low	Struggles with dynamic,

based	threats)		evolving machine behaviors
Statistical	Moderate	Moderate	Can detect simple anomalies, but may generate false positives
Behavioral	High	Moderate	Effective for profiling user behavior; needs tuning for machine entities
ML-based	High	High	Learns complex patterns in both; best with sufficient labeled data

5.7. Compliance and Policy Enforcement at Scale

Compliance with data protection regulations and internal policies becomes more difficult when dealing with thousands of dynamic, autonomous identities. Key concerns include:

- How to log, audit, and report on non-human entity actions
- Mapping machine activities to regulatory frameworks (e.g., GDPR, HIPAA)
- Defining access policies that remain consistent across cloud, edge, and hybrid environments

Without robust governance frameworks, organizations face increased risk of both security breaches and compliance violations.

Securing non-human entities is not simply an extension of human identity management; it requires a new paradigm that emphasizes automation, distributed trust, and adaptive intelligence. Addressing the challenges outlined in this section will be central to the development of secure and resilient machine-to-machine communication infrastructures. The path forward lies in unifying identity standards, integrating automated credential management, and embedding AI-driven monitoring at scale.

6. Future Directions and Recommendations

As non-human identities become central actors in digital ecosystems, securing machine-to-machine (M2M) communications must evolve beyond current reactive approaches. The future of cybersecurity for autonomous systems, IoT devices, and APIs demands innovations in identity governance, architecture design, and intelligent threat detection. This section outlines strategic research directions and actionable recommendations for building scalable, adaptive, and secure M2M environments.

6.1. Establishing Machine Identity Governance (MIG) Frameworks

A key future priority is the development of comprehensive Machine Identity Governance (MIG) frameworks. These would define policies and procedures for:

- Machine identity issuance, renewal, and revocation
- Credential lifecycle management (including rotation and expiry)
- Role-based access control tailored to non-human entities
- Compliance auditing and accountability tracking

Such frameworks must be flexible enough to support heterogeneous devices and protocols while ensuring security at scale.

6.2. AI/ML for Behavioral Anomaly Detection

Traditional rule-based systems are insufficient for the dynamic nature of M2M traffic. Future solutions will increasingly rely on AI/ML models to:

- Profile baseline behaviors of machine identities
- Detect anomalies in communication patterns or device behavior
- Predict malicious activity based on real-time telemetry

Unsupervised learning models (e.g., autoencoders, clustering algorithms) can be particularly effective where labeled datasets are scarce. Additionally, online learning systems can adapt to concept drift, a common occurrence in high-velocity M2M environments.

6.3. Decentralized Identity (DID) and Blockchain Integration

Emerging technologies like Decentralized Identifiers (DIDs) and blockchain offer promising avenues for reducing reliance on centralized identity providers:

- Devices can generate and control their own identities (self-sovereign identity)
- Blockchain can serve as a tamper-proof registry for machine credentials and trust relationships
- Smart contracts can automate identity verification, access grants, and revocations

While still in experimental stages, these technologies may offer scalable trust frameworks suitable for highly distributed M2M ecosystems.

6.4. Zero Trust Architectures for M2M

Future-ready M2M environments must move beyond implicit trust models by adopting Zero Trust Architecture (ZTA) principles:

- “Never trust, always verify” applies to every machine, API, and service
- Continuous authentication and micro-segmentation of networks
- Enforcement of least-privilege access through context-aware policies

ZTA helps contain breaches and limit lateral movement even when one device or service is compromised. Implementing zero trust in automated environments requires tight integration between identity providers, access control engines, and runtime behavioral monitoring.

6.5. Secure Bootstrapping and Edge-Aware Authentication

For edge computing and IoT contexts, secure onboarding and bootstrapping of devices remain a major hurdle. Future approaches should enable:

- Lightweight cryptographic protocols (e.g., EDHOC, ACE-OAuth) for constrained environments
- Identity attestation at hardware and firmware levels
- Remote attestation and hardware root of trust (e.g., TPM, TEE)

These mechanisms must be streamlined for millions of devices, many of which have limited memory, processing, and energy resources (Vummadi & Hajarath, 2021).

6.6. Standardization and Regulatory Alignment

The lack of universal standards for machine identity and M2M authentication remains a significant barrier. Future research and industry efforts must focus on:

- Harmonizing efforts across organizations (IETF, W3C, NIST, ISO)
- Aligning identity protocols with privacy laws (e.g., GDPR, HIPAA)
- Creating certification schemes for machine identity providers and IoT vendors

Governance models must balance security, performance, and regulatory compliance while preserving interoperability across ecosystems.

The security of M2M communications in a world dominated by non-human identities demands a proactive, multi-layered approach that combines governance, automation, and intelligent monitoring. Future success hinges not only on the development of new protocols and algorithms but also on establishing trust, visibility, and accountability across all layers of machine interaction. By investing in these strategic areas, stakeholders can build resilient infrastructures that are both secure and scalable in the face of growing complexity.

7. Conclusion

With the digital age, the machine-to-machine (M2M) interaction has experienced a rise like never before which has basically altered communication between systems, services, and devices. This transformation has introduced yet another new generation to actors who are not human identity that have the ability to act without external control and carry out significant roles within the cloud environments, IoT, APIs, and autonomous systems. Since the number of them increases, the stronger the pressure to get them.

This paper has discussed the complex nature of the challenges that face the security of non-human entities, In the form of concerns of identity lifecycle management, credential rotation, trust modeling, visibility and compliance. It has also studied existing solutions/norms, which include PKI, OAuth 2.0, and Zero Trust Architecture, providing a decent (yet incomplete) set of solutions in this emergent problem area.

The fact is that current security paradigms which have traditionally been developed upon human based authentication and access schemes are not enough as dynamic, large scale and dispersed M2M ecosystems are concerned. Non-human identities also present challenges and require greater than technical innovation: architectural and regulatory change as well. Lack of proactive governance would also make these channels an Achilles heel in the enterprise security strategy.

In the future, organizations require computer-first identity strategy, which focuses on automated, ongoing trust assessment, credential short-lived, and real-time behavioral insight. Meanwhile, a combined industry and standardization initiative is necessary to achieve interoperable system development and scalable policy to maintain the changing technology at the same time.

To sum up, M2M communications in our times of non-human identities are not only a requirement of a technical character but also of a key pillar of cyber resilience in our modern digital world. Guaranteeing confidence, visibility and control of machine entities will be paramount in defending the infrastructures of tomorrow today.

References

1. Verma, P. K., Verma, R., Prakash, A., Agrawal, A., Naik, K., Tripathi, R., ... & Abogharaf, A. (2016). Machine-to-Machine (M2M) communications: A survey. *Journal of Network and Computer Applications*, *66*, 83-105.
2. Lucic, D., Caric, A., & Lovrek, I. (2015, July). Standardisation and regulatory context of machine-to-machine communication. In *2015 13th International Conference on Telecommunications (ConTEL)* (pp. 1-7). IEEE.
3. Gapsevicius, M. (2016). *An Artistic Perspective on Distributed Computer Networks. Creativity in Human-Machine Systems* (Doctoral dissertation, Goldsmiths, University of London).
4. Demblewski, M. (2015). *Security frameworks for machine-to-machine devices and networks* (Doctoral dissertation, Nova Southeastern University).
5. Williamson, G., Koot, A., & Lee, G. (2022). Non-human Account Management (v4). *IDPro Body of Knowledge*, *1*(11).
6. Chaudhary, R., Jindal, A., Aujla, G. S., Aggarwal, S., Kumar, N., & Choo, K. K. R. (2019). BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system. *Computers & Security*, *85*, 288-299.
7. Houhamdi, Z., & Athamena, B. (2020). Identity identification and management in the internet of things. *Int. Arab J. Inf. Technol.*, *17*(4A), 645-654.
8. Nuss, M., Puchta, A., & Kunz, M. (2018, July). Towards blockchain-based identity and access management for internet of things in enterprises. In *International Conference on Trust and Privacy in Digital Business* (pp. 167-181). Cham: Springer International Publishing.
9. Vaidya, R., Yadav, C., Kunkumath, J., & Yadati, P. (2011, December). Network congestion control: Mechanisms for congestion avoidance and recovery. In *Proceedings of the 1st International Conference on Wireless Technologies for Humanitarian Relief* (pp. 199-207).
10. Leiding, B. (2019). *The M2X Economy–Concepts for Business Interactions, Transactions and Collaborations Among Autonomous Smart Devices* (Doctoral dissertation, Dissertation, Göttingen, Georg-August Universität, 2019).
11. Jöhnk, J., Albrecht, T., Arnold, L., Guggenberger, T., Lämmermann, L., Schweizer, A., & Urbach, N. (2021, July). The Rise of the Machines: Conceptualizing the Machine Economy. In *PACIS* (p. 54).
12. Jöhnk, J., Albrecht, T., Arnold, L., Guggenberger, T., Lämmermann, L., Schweizer, A., & Urbach, N. (2021, July). The Rise of the Machines: Conceptualizing the Machine Economy. In *PACIS* (p. 54).
13. Ulgen, O. (2017). Kantian ethics in the age of artificial intelligence and robotics. *QIL*, *43*, 59-83.

14. Murynets, I., & Piqueras Jover, R. (2012, November). Crime scene investigation: SMS spam data analysis. In *Proceedings of the 2012 Internet Measurement Conference* (pp. 441-452).
15. Verma, A., Khanna, A., Agrawal, A., Darwish, A., & Hassanien, A. E. (2019). Security and privacy in smart city applications and services: Opportunities and challenges. *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*, 1-15.
16. Hildebrandt, M. (2008). Defining profiling: A new type of knowledge?. In *Profiling the European citizen: Cross-disciplinary perspectives* (pp. 17-45). Dordrecht: Springer Netherlands.
17. Machin, J., Batista, E., Martinez-Balleste, A., & Solanas, A. (2021). Privacy and security in cognitive cities: A systematic review. *Applied Sciences*, *11*(10), 4471.
18. Vummadi, J. R., & Hajarath, K. C. R. (2021).AI and Big Data Analytics for Demand-Driven SupplyChain Replenishment. Educational Administration: Theory and Practice, 27 (1), 1121–1127.

19. Beck, E. (2016). A theory of persuasive computer algorithms for rhetorical code studies. *Enculturation, 23*.