Interdisciplinary Journal of Global and Multidisciplinary
IJGAM
ISSN xxxx-xxxx
+62852-3430-9925 https://jurnal-ijgam.or.id/ admin@jurnal-ijgam.or.id
Diterbitkan Oleh PT. RADJA POS MEDIA
Vol. 2, No. 1, January 2026 | Page. 763 - 773

THE ROLE OF CRYPTOGRAPHY IN DATA SECURITY FOR THE INTERNET OF THINGS (IOT)

Taufik Hidayat[1], Ibnu Rusydi[2]
Faculty of Science and Technology,
State Islamic University of North Sumatra, Indonesia
Email: taufikk2500@gmail.com, ibnurusydi@dharmawangsa.ac.id

Keywords:
Cryptography,
Internet of Things,
Data Security,
Key Management.

Abstrak

The Internet of Things (IoT) has become a foundational layer of modern digital infrastructure, connecting consumer devices, industrial sensors, smart cities, healthcare wearables, and critical systems. As adoption accelerates, the attack surface expands: IoT devices often operate with constrained CPU, memory, and power, yet they continuously generate and exchange sensitive data. Recent market tracking estimates that connected IoT devices reached about 18.5 billion in 2024 and are projected to grow to 21.1 billion in 2025, highlighting the scale at which security mechanisms must function reliably. In parallel, security telemetry and threat research show sustained exploitation of weak authentication, outdated firmware, insecure default configurations, and unencrypted communications conditions frequently leveraged by botnets and large-scale denial-of-service campaigns. This paper examines the role of cryptography as a primary control for confidentiality, integrity, authentication, and non-repudiation in IoT ecosystems. It also considers how cryptography must be implemented holistically supported by key management, secure update mechanisms, and device lifecycle governance to remain effective in real-world deployments. Using a qualitative descriptive internet-based study approach, this work synthesizes recent standards guidance and threat landscape reporting, including NIST's updated foundational IoT cybersecurity activities and ENISA's threat landscape framing. The discussion organizes cryptographic practices across device, network, and cloud layers, and evaluates common trade-offs such as computational cost, latency, usability, and maintainability. The findings emphasize that cryptography is necessary but insufficient alone; it must be integrated with secure-by-design engineering, robust identity, and operational monitoring to protect IoT data at global scale.

INTRODUCTION

The Internet of Things (IoT) refers to a growing ecosystem of connected devices sensors, actuators, gateways, and embedded systems—that communicate over networks to collect data and automate actions. IoT adoption has accelerated in consumer environments (smart homes, cameras, wearables), enterprise settings (asset tracking, smart buildings), and industrial contexts (SCADA/ICS, predictive maintenance). This expansion delivers significant benefits: real-time visibility, efficiency gains, automation, and improved service delivery. However, the same connectivity that enables value also amplifies security risks. Each device becomes a potential entry point into a network, and each data stream can expose sensitive operational or personal information.

The scale of IoT growth is central to the security challenge. Recent industry tracking indicates that connected IoT devices reached approximately 18.5 billion in 2024 and are expected to reach 21.1 billion by the end of 2025, with longer-term projections climbing far beyond that. This growth creates two intertwined pressures. First, the volume of endpoints makes traditional perimeter security insufficient; security must be distributed, automated, and resilient. Second, heterogeneous device capabilities and vendors lead to inconsistent security baselines, uneven patching practices, and widely varying cryptographic maturity.

IoT data is valuable and often sensitive. Consumer IoT can reveal behavioral patterns, home occupancy, audio/video content, and geolocation. Industrial IoT can expose proprietary production metrics, safety-relevant control parameters, and operational continuity. In healthcare, wearables and connected medical devices may involve protected health data and safety-critical functionality. When attackers compromise IoT data flows, consequences can range from privacy breaches and fraud to physical safety incidents and major service outages.

Threat research repeatedly links IoT insecurity to large-scale disruption. Botnets commonly recruit poorly secured devices such as routers and IP cameras, then leverage them for DDoS attacks and other criminal operations. Trend Micro reported monitoring large-scale DDoS activity driven by an IoT botnet exploiting vulnerable devices since late 2024, illustrating the persistence and automation of these campaigns. Complementing this, the Bitdefender IoT security landscape analysis examined tens of millions of devices and billions of security events, underscoring how frequently consumer IoT is exposed to malicious scanning, exploitation attempts, and misconfiguration risks. These patterns reflect a broader reality: IoT security weaknesses are not isolated edge cases but systemic issues influenced by cost constraints, fragmented supply chains, and long device lifecycles.

Within this context, cryptography plays a pivotal role. Cryptography provides the mathematical foundations for protecting data confidentiality (preventing unauthorized disclosure), ensuring integrity (detecting tampering), enabling authentication (verifying identities of devices and services), and supporting non-repudiation (proof of origin through signatures). For IoT, these properties are essential because devices frequently communicate over untrusted networks and operate in physically accessible environments where attackers may attempt hardware-level tampering or credential extraction.

Yet IoT cryptography faces distinctive constraints. Many devices operate with limited battery life, limited compute resources, and minimal memory. Some must function with intermittent connectivity. Others are deployed in remote or harsh environments and may remain in service for a decade or more. Cryptographic controls must therefore be efficient, implementable across varied platforms, and maintainable through updates over time. Additionally, cryptography's effectiveness depends on secure key management how keys are generated, stored, rotated, revoked, and recovered. Weak key provisioning, reuse of default keys, or insecure storage can neutralize even strong algorithms.

Another key issue is governance and baseline requirements. Security guidance increasingly emphasizes "secure-by-design" principles and lifecycle cybersecurity activities for IoT product manufacturers. NIST's foundational guidance for IoT manufacturers highlights recommended activities to reduce compromise prevalence and severity, focusing on making products more securable and ensuring customers receive essential cybersecurity functionality and information. Meanwhile, ENISA's threat landscape reporting highlights major categories of cyber threats such as ransomware and availability attacks reinforcing that IoT ecosystems are part of a broader threat environment where data and service disruption are central attacker goals. These perspectives imply that cryptography is not just a technical feature but a core component of product security strategy and risk management.

This paper focuses on the role of cryptography in IoT data security by addressing several guiding questions: (1) What are the primary IoT security risks that cryptography can mitigate? (2) Which cryptographic mechanisms are most relevant across device, network, and cloud layers? (3) How do constraints (performance, power, usability, lifecycle support) shape cryptographic design choices? and (4) What supporting controls especially key management and secure updates are required to make cryptography effective in practice?

The significance of this topic lies in the real-world gap between theory and deployment. Strong algorithms are widely available, but implementation mistakes, poor credential hygiene, and insufficient lifecycle support remain common. Many IoT incidents stem from failures such as hardcoded passwords, missing encryption in telemetry, insecure pairing processes, or unverified firmware updates. By synthesizing recent guidance and threat observations, this study aims to provide a structured understanding of how cryptography should be positioned within IoT security architecture what it can reliably provide, where it fails without operational support, and how organizations can prioritize cryptographic controls to reduce risk.

Ultimately, the role of cryptography in IoT is foundational but must be treated as part of a system: identity, keys, secure boot, update trust, and monitoring all interact. When integrated correctly, cryptography enables trustworthy data exchange at massive scale. When integrated poorly, it can create a false sense of security. The sections that follow review relevant literature, describe the research method, discuss findings across key IoT security domains, and conclude with practical implications for IoT stakeholders.

LITERATURE REVIEW

Cryptography Fundamentals for IoT Security

Cryptography is the discipline that enables secure communication and trustworthy computing in adversarial environments. In IoT, cryptography primarily supports four goals: confidentiality (encryption), integrity (hashing and message authentication), authentication (proof of identity), and non-repudiation (digital signatures). Symmetric encryption (e.g., AES) is commonly used for efficient data confidentiality, while asymmetric cryptography (e.g., ECC, RSA) supports scalable identity and trust through public-key infrastructure (PKI). IoT environments often prefer elliptic-curve cryptography due to efficiency advantages on constrained hardware.

However, cryptography is not merely algorithm selection; it depends on correct implementation and operational handling of secrets. Weak randomness, poor key derivation, improper certificate validation, or insecure storage can undermine cryptographic assurances. IoT devices are also frequently deployed in physically accessible places, raising the risk of key extraction through hardware attacks. This means cryptographic design must consider secure elements, trusted execution environments, or other protections to safeguard long-term keys.

From a systems perspective, cryptography underpins secure protocols (e.g., TLS/DTLS), secure pairing, and device-to-cloud trust. It also supports firmware signing for supply chain integrity and safe updates. Because IoT devices often remain deployed for long periods, cryptographic agility (ability to upgrade algorithms and rotate keys) is essential for resilience as threats evolve. The literature emphasizes that cryptography provides strong security properties when combined with governance and lifecycle practices that ensure keys, identities, and updates remain controlled over time.

IoT Threat Landscape and the Need for Cryptographic Controls

IoT threats frequently exploit weak authentication, unencrypted communications, exposed services, and delayed patching. Botnets that compromise routers, cameras, and similar devices can transform insecure endpoints into infrastructure for disruptive attacks. Research monitoring large-scale DDoS campaigns tied to IoT botnets highlights how attackers leverage vulnerable devices at scale, particularly when default credentials, outdated firmware, or exposed management interfaces remain unaddressed. At the same time, large-scale security telemetry studies emphasize that consumer IoT environments generate massive volumes of suspicious activity, suggesting persistent scanning and exploitation attempts in the wild.

Broader threat landscape reporting also contextualizes IoT within the global cyber ecosystem. ENISA identifies major threat categories and emphasizes the continued prominence of availability attacks and ransomware, which can involve IoT either as an entry point or as an amplification layer. As the number of connected devices grows rapidly, the probability of misconfiguration and unpatched vulnerabilities increases, creating an environment where attackers can reliably find weak targets.

Within this landscape, cryptographic controls are essential for reducing key attack opportunities. Strong authentication mechanisms (certificate-based identities, mutual TLS) reduce the effectiveness of credential stuffing and default-password exploitation. Encryption reduces the value of intercepted telemetry and blocks straightforward eavesdropping on device communications. Signed firmware and secure boot reduce supply chain manipulation and unauthorized code execution. The literature consistently frames cryptography as a core technical safeguard, especially where

network trust cannot be assumed.

Standards and Guidance for IoT Security-by-Design

Standards bodies and government institutions increasingly promote IoT security-by-design, emphasizing that manufacturers should embed cybersecurity capabilities into products rather than shifting responsibility entirely to end users. NIST's foundational guidance for IoT product manufacturers describes recommended pre-market cybersecurity activities aimed at reducing compromise prevalence and severity and improving the "securability" of IoT products. While such guidance covers multiple control categories, cryptography is implicitly central to secure communications, identity, and update integrity.

Security-by-design literature stresses the importance of default-secure configurations, elimination of hardcoded credentials, secure onboarding, and patchability. Cryptography supports these objectives by enabling secure provisioning (unique device identities), secure communications (encryption and integrity protection), and secure updates (digital signatures). Yet standards also highlight that cryptography must be manageable: keys and certificates must be uniquely assigned, stored securely, and rotated when compromised or expired.

In addition, standards-aligned approaches emphasize transparency and customer enablement providing the information and controls needed for secure operation. In practice, this includes documenting supported cipher suites, update mechanisms, certificate handling, and expected lifecycle support. Standards-based literature also encourages alignment with organizational risk management frameworks, where cryptography is treated as a control with measurable objectives (e.g., encryption coverage, certificate expiration monitoring, update signature verification rates). Overall, standards guidance strengthens the argument that cryptography should be planned as part of the product lifecycle, not bolted on after deployment.

Key Management and Trust Models in IoT Architectures

Key management is often the decisive factor in whether cryptography actually protects IoT systems. IoT architectures involve multiple trust relationships: device-to-device, device-to-gateway, device-to-cloud, and cloud-to-operator. Each relationship requires secure identity proofing, credential issuance, storage, and renewal. Typical trust models include PKI (certificates), pre-shared keys (PSKs) for constrained settings, and token-based authorization layered above cryptographic channels.

The literature highlights recurring key management failures: reused default keys across device fleets, keys stored in plaintext firmware, insecure factory provisioning, and inadequate revocation processes. These failures allow attackers to compromise large numbers of devices using a single extracted secret. By contrast, robust models employ unique per-device keys, hardware-backed storage (secure elements), and automated certificate lifecycle management (issuance, rotation, revocation). At scale, automation becomes essential because billions of devices cannot be managed manually.

Another theme is lifecycle trust continuity: a device must remain trustworthy from manufacturing to decommissioning. That implies secure onboarding (identity verification at first connection), authenticated configuration changes, signed updates, and controlled end-of-life processes (key destruction, certificate revocation). Key management also intersects with privacy: rotating identifiers and using ephemeral session keys can reduce linkability and data exposure.

In summary, the literature positions key management as the "operational spine" of cryptography in IoT. Without secure provisioning and lifecycle maintenance, encryption and signatures may exist but fail to deliver practical security outcomes.

RESEARCH METHOD

This study uses a descriptive qualitative approach with an internet-based literature study design to examine how cryptography contributes to IoT data security. The qualitative descriptive method is appropriate because the research objective is not to test a single causal hypothesis, but to compile, interpret, and categorize contemporary knowledge from credible sources into a coherent explanation of cryptography's roles, limitations, and implementation requirements in IoT ecosystems.

Data Sources and Selection

Data were collected from publicly available internet sources, focusing on: (1) international standards and government publications addressing IoT cybersecurity practices; (2) reputable threat landscape and incident analyses from recognized security organizations; and (3) recent industry research on IoT adoption trends. Priority was given to sources published within the last one to two years to reflect current IoT scale and evolving threats, including NIST guidance on foundational IoT cybersecurity activities and ENISA's threat landscape framing of major threats , as well as IoT growth tracking that contextualizes the magnitude of endpoints. Additional threat context was drawn from security research documenting IoT botnets and widespread IoT security telemetry.

Inclusion criteria were: relevance to IoT security and cryptography; clarity of methodology or organizational credibility; and information that can be triangulated with at least one other reputable source (e.g., standards aligned with observed threats). Exclusion criteria included: anonymous blog claims without evidence, duplicated content, or sources that did not clearly separate facts from speculation.

Data Collection and Analysis Procedure

The analysis followed three steps. First, sources were read and coded to extract recurring concepts: confidentiality, integrity, authentication, authorization, key management, secure boot, firmware validation, and lifecycle security. Second, the codes were grouped into thematic categories that align with IoT architecture layers (device, network, cloud) and operational lifecycle phases (provisioning, deployment, maintenance, decommissioning). Third, the findings were synthesized into descriptive explanations that connect threat patterns (e.g., botnets exploiting weak credentials) with cryptographic controls (e.g., certificate-based device identity, encrypted telemetry, signed firmware updates). To improve trustworthiness, the study applied qualitative triangulation by comparing claims across different types of sources (standards vs. threat reports vs. market tracking). The output is an integrated narrative of how cryptography should be implemented in IoT, emphasizing practical dependencies such as secure key storage and update integrity.

RESULT AND DISCUSSION

Cryptography for Confidentiality of IoT Data in Transit and at Rest

A major result of this synthesis is that confidentiality in IoT must be treated as an end-to-end property, not merely an optional feature of network transport. IoT data often travels from device sensors to gateways, then to cloud services and analytics

platforms. If any segment is transmitted without encryption, attackers can capture meaningful information through passive monitoring or compromise intermediate infrastructure. At massive scale over 18.5 billion connected devices in 2024 and rising unencrypted telemetry can produce systemic privacy and operational risks.

Encryption in transit typically relies on TLS or DTLS, depending on whether the device uses TCP or UDP. For constrained environments, lightweight secure transports and optimized cipher suites are necessary to limit CPU and energy overhead. Confidentiality at rest is equally important because devices may store local logs, credentials, or cached sensor data. Attackers who gain physical access can extract storage contents if not protected, while attackers who gain remote access may exfiltrate local databases. Therefore, encryption at rest should be paired with hardware-backed key storage when feasible.

However, the discussion also reveals trade-offs. Strong encryption without appropriate key management is fragile: if keys are hardcoded or reused, confidentiality collapses at fleet scale. Additionally, some IoT deployments prioritize uptime and low latency, leading teams to disable encryption or use outdated cipher configurations. This is particularly risky in industrial and healthcare settings where data can be safety-relevant. A practical implication is that organizations should define minimum encryption baselines by device class. For example: always encrypt external communications, require modern cipher suites, rotate session keys, and store long-term keys in secure elements. Where resource constraints are extreme, designs should still enforce integrity and authentication at minimum, while using efficient symmetric encryption for payload protection.

Authentication and Device Identity: From Passwords to Certificates

A second key result is that authentication failures remain one of the most common enablers of IoT compromise. Botnets frequently rely on weak credentials, exposed services, and predictable access patterns. The persistence of IoT-driven DDoS activity linked to exploitation of vulnerable routers and cameras indicates that many devices still fail at basic identity assurance and access control. Cryptography strengthens authentication by enabling scalable, verifiable identities. Certificate-based device identity (PKI) supports mutual authentication: devices authenticate servers, and servers authenticate devices. This reduces reliance on shared secrets and weak passwords, and it enables centralized lifecycle management (expiration, renewal, revocation). In contrast, default passwords and shared credentials create “single point of fleet failure,” where one leaked secret compromises many devices.

Yet certificate-based models introduce operational complexity. Manufacturers and operators must manage certificate issuance during production or provisioning, protect private keys on-device, and implement renewal processes that work reliably under intermittent connectivity. The literature and guidance emphasize the importance of designing for securability meaning device identity and credential handling should be feasible for customers to operate securely, not merely theoretically secure. NIST’s foundational IoT cybersecurity activities reinforce the broader need for manufacturers to reduce customer burden by embedding appropriate security functionality and information into IoT products. In practice, a hybrid approach is common: devices use asymmetric cryptography for identity bootstrapping and secure session establishment, then switch to efficient symmetric keys for ongoing communication. Strong authentication should also be paired with least-privilege authorization (what a device is

allowed to do after it authenticates). Overall, the findings highlight that upgrading authentication is one of the highest-impact security improvements in IoT often more impactful than adding new analytics because it prevents mass exploitation and improves incident containment.

Integrity, Secure Boot, and Signed Firmware Updates

The third result concerns integrity as a prerequisite for trustworthy IoT operation. Even when data is encrypted, compromised firmware can leak data, falsify sensor readings, or sabotage device function. Integrity must therefore apply to both data and code. Cryptographic hashing and message authentication codes (MACs) protect data integrity in transit, while digital signatures protect software integrity across the device lifecycle.

Signed firmware updates are particularly critical because IoT devices often receive patches remotely. Without signature verification, attackers can push malicious updates, persist in devices, and spread laterally. Secure boot extends this concept by ensuring that devices only run firmware that is cryptographically verified at startup. This reduces the risk of low-level persistence and supply chain compromise.

Threat landscape reporting underscores that availability and data threats remain prominent; IoT devices can be targets themselves or leveraged as a means to disrupt others. In that environment, integrity controls help prevent attackers from turning devices into "weapons" (botnets) or from degrading services through malicious reconfiguration.

However, integrity mechanisms face two implementation risks. First, weak key protection: if signing keys are compromised, signatures become meaningless. Second, update process fragility: failed updates can brick devices, leading teams to avoid frequent patching. This creates a paradox where security is known to be needed but operational risk discourages updates.

A balanced design includes: separated signing keys (offline root keys), staged rollout, rollback protection, and transparent update logging. Integrity is also strengthened by vulnerability disclosure programs and consistent lifecycle support. The synthesis indicates that cryptography enables integrity, but organizations must invest in secure update infrastructure and governance to realize its benefits.

Cryptography vs. Constraints: Performance, Energy, and Usability Trade-offs

A consistent finding is that IoT cryptography must be engineered under constraints that differ from traditional IT systems. Devices may be battery-powered and must preserve energy; they may use low-bandwidth networks; and they may have limited CPU cycles for handshake protocols. As the number of devices increases toward tens of billions, even small inefficiencies multiply into significant cost and operational burden.

This leads to real trade-offs. Strong asymmetric operations are computationally heavier than symmetric encryption; frequent handshakes may impact latency; and certificate validation may require memory and time. As a result, some implementations choose weaker approaches such as PSKs with poor rotation or disable verification to "make it work," inadvertently undermining security. The research literature typically recommends using efficient primitives (e.g., elliptic-curve cryptography) and session resumption, and minimizing expensive operations while preserving authentication and integrity guarantees.

Usability is another constraint. Many IoT compromises occur not because

cryptography is unavailable, but because it is difficult to configure correctly. If device onboarding is complex, users may leave default credentials or skip updates. If certificate management is poorly documented, operators may bypass validation. This aligns with the secure-by-design viewpoint that manufacturers should provide cybersecurity functionality and information that reduce customer burden.

An important practical approach is profiling devices into classes: constrained sensors, consumer smart devices, gateways, and cloud components. Each class can adopt a tailored cryptographic baseline. For example: sensors use lightweight secure transport and symmetric payload encryption, gateways perform heavier certificate operations, and cloud services enforce strict policies and monitoring. The discussion concludes that cryptography is feasible across IoT but only if designs match device constraints and reduce operational friction through automation and good defaults.

Governance, Compliance, and the "Cryptography Is Not Enough" Principle

The final result is that cryptography is necessary but not sufficient. Organizations often assume that "adding encryption" solves IoT security, but real-world incidents show that failures in identity, patching, configuration, and monitoring can bypass cryptographic controls. Telemetry-based security studies illustrate the sheer volume of suspicious activity targeting IoT, meaning defenses must be layered and continuously validated.

Governance matters because IoT devices are long-lived and may outlast the teams or vendors that deployed them. Policies must define who owns certificates, how revocation is handled, how keys are rotated, and what happens when a vendor ends support. Standards and threat landscape reporting support the need for structured risk management: ENISA's emphasis on major threat categories (including availability and ransomware) reinforces that organizations must plan for resilience and incident response, not only prevention. Likewise, NIST's foundational guidance indicates that manufacturers should reduce customer burden by embedding cybersecurity activities and providing the information customers need an approach that indirectly strengthens cryptographic effectiveness by improving lifecycle maintainability.

A governance-driven cryptography program typically includes: a device identity strategy, cryptographic agility planning, secure update infrastructure, vulnerability management, asset inventory, and monitoring for anomalous behavior. It also includes procurement requirements demanding that vendors support modern protocols, unique credentials, and long-term patching. Therefore, the role of cryptography should be framed as a cornerstone within a broader security architecture. When governance, lifecycle support, and operational monitoring are strong, cryptography enables scalable trust. When they are weak, cryptography becomes an isolated feature that may not reduce actual risk.

CONCLUSION

This study concludes that cryptography is a foundational mechanism for IoT data security because it enables confidentiality, integrity, and authentication across device, network, and cloud layers. As IoT adoption expands to tens of billions of devices, cryptography becomes even more essential to prevent passive interception, tampering, impersonation, and malicious firmware manipulation. Market tracking showing IoT growth from about 18.5 billion devices in 2024 to an expected 21.1 billion in 2025 illustrates why scalable, automated cryptographic controls are required.

However, the effectiveness of cryptography depends on correct implementation and strong key management throughout the device lifecycle. Threat research documenting IoT botnets exploiting vulnerable routers and cameras reinforces that weak identity and poor credential hygiene can negate cryptographic protections. Standards guidance, such as NIST's foundational IoT cybersecurity activities, supports the need for security-by-design that reduces customer burden and improves device securability. In practical terms, cryptography should be deployed together with secure provisioning, hardware-backed key storage where feasible, signed updates, secure boot, and governance processes for rotation and revocation. Cryptography is not a complete solution by itself, but when integrated into a layered security program, it provides the trust foundation needed for safe and reliable IoT at global scale.

BIBLIOGRAPHY

Alfatah, D. (2024). Penggunaan Kriptografi Asimetris dalam Pengamanan Komunikasi IoT. *Jurnal Komputer*, *3*(1), 19-24.

Anggono, S. U., Siswanto, E., & Fajri, L. R. H. A. (2023). User interface berbasis web pada perangkat Internet of Things. *Teknik: Jurnal Ilmu Teknik dan Informatika*, *3*(1), 35-54.

Febrianto, R. W., & Zulianto, A. (2024). Kriptografi Ringan dengan Menggunakan Algoritma di Internet Of Things (IoT). *Journal of Informatics Management and Information Technology*, *4*(3), 81-91.

Hidayat, T., & Fergina, A. (2025, May). Implementasi Enkripsi Data End-to-End pada Komunikasi Perangkat IoT Berbasis Lightweight Cryptography. In *Prosiding Seminar Nasional Teknologi Informasi, Mekatronika, dan Ilmu Komputer* (Vol. 4, pp. 25-29).

Irawan, B. (2023). Implementasi teknologi blockchain untuk keamanan data internet of things. *Humantech: Jurnal Ilmiah Multidisiplin Indonesia*, *2*(9), 1944-1953.

Leba, C. K. R. (2025). PERAN INTERNET OF THINGS DALAM MENINGKATKAN KEAMANAN DAN EFISIENSI TRANSPORTASI. *Elektrika*, *17*(1), 26-31.

Maldini, R. R. (2023). Sistem Keamanan Teknologi untuk Sistem Internet of Thing. *Bandung: Universitas Komputer Indonesia. Sumber: https://www. researchgate. net/publication/370074375*.

Muhana, M. F., & Fuad, E. (2024). Keamanan Dan Implementasi IoT Dalam Lingkungan Industri. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(4), 7848-7855.

Pradana, A., Mahayana, D., & Rosmansyah, Y. (2024). Keamanan Data Internet of Things dalam Perspektif Pseudosains Mario Bunge: Internet of Things Data Security in Mario Bunge's Pseudoscience Perspective. *Jurnal Filsafat Indonesia*, *7*(2), 207-216.

Ramadan, A. R., & Prakoso, A. W. (2020). Implementasi Kriptografi AES untuk Keamanan Pengiriman Data Internet of Things Menggunakan Web Service Rest pada NodeMCU. *Systemic: Information System and Informatics Journal*, *6*(1), 1-6.

Rivai, A. M., Febisatria, A., Sarnawiyah, T., & Setiawan, M. R. (2025). INTERNET OF THINGS (IoT) SEBAGAI PILAR KEAMANAN DATA PADA SISTEM DISTRIBUSI DI INDONESIA. *Jurnal Ilmiah Ekonomi Dan Manajemen*, *3*(12), 332-341.

Saputra, R. A., Ridwansyah, R. D., Erlangga, D. A., & Rilvani, E. (2025). KEAMANAN SISTEM OPERASI DALAM ERA INTERNET OF THINGS. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(2), 1939-1944.

Simbolon, A. B., Anjelita, A., Purba, D. C., Febrina, D., Hutasuhut, I. F., Harahap, I. G., ... & Sipahutar, S. J. M. (2025). Pengantar Sistem Keamanan pada Internet of Things. *Tangguh Denara Jaya Publisher*.

Wulan, W., Hadita, H., Fauzi, A., Putri, A. M., Fitriyani, F., Astriyani, R., ... & Cahyani, Y. I. (2024). Tinjauan Ancaman dan Risiko pada Sistem Keamanan Internet of Things, Berbasis Cloud Computing dalam Penggunaan E-Commerce dan Rencana Strategis. *Jurnal Kewirausahaan dan Multi Talenta*, *2*(2), 126-137.