Babylonian Journal of Internet of Things
Vol.2026, **pp**. 187–196
DOI: https://doi.org/10.58496/BJIoT/2026/012; ISSN: 3006-1083
https://mesopotamian.press/journals/index.php/BJIoT

Research Article

AI-Powered Trust Management and Cryptographic Access Control in IoT Systems

Dhuha Al-Adhami [1,*], Hamza Gharsellaoui[2], Olfa Belkahla Driss [3]

[1] *Faculty of Sciences of Tunis, University of Tunis El Manar, Tunis, Tunisia.*

[2] *National School of Computer Science (ENSI), University of Manouba, Manouba, Tunisia.*

[3] *ESCT, University of Manouba, Manouba 2010, Tunisia.*

ARTICLE INFO

Article History

Received 30 Apr 2026
Revised 18 May 2026
Accepted 30 Jun 2026
Published 23 Jul 2026

Keywords
AI,
Cryptographic,
Internet of Things,
Access Control,
Security,
Privacy.

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and innovation across various sectors such as healthcare, smart cities, and industrial automation. However, this pervasive integration also introduces significant security, privacy, and trust challenges, primarily due to the decentralized, dynamic, and resource-constrained nature of IoT ecosystems. Ensuring secure and reliable interactions among heterogeneous devices and users is paramount for the successful deployment and adoption of IoT technologies. This paper comprehensively reviews AI-powered trust management and cryptographic access control mechanisms designed to address these critical issues in IoT systems. We explore the fundamental principles, advanced techniques, and the synergistic integration of AI and cryptography to enhance security, privacy, and trustworthiness. Drawing upon recent research from 2023 to 2026, we analyze the strengths, limitations, and practical implications of various solutions, including AI-driven anomaly detection, federated learning, homomorphic encryption, and blockchain-based trust models. Furthermore, we identify emerging trends, future directions, and persistent challenges such as scalability, interoperability, and ethical considerations, offering a holistic perspective on the evolving landscape of secure IoT. The aim is to synthesize current knowledge and highlight key research avenues for developing more robust, adaptive, and context-aware security frameworks for future IoT environments.

1. INTRODUCTION

The Internet of Things (IoT) has transformed everyday objects into interconnected entities capable of collecting, exchanging, and processing data in real-time. This paradigm shift has enabled significant advancements in diverse applications, from continuous patient monitoring in healthcare to optimized energy consumption in smart cities [1]. Despite the immense potential, the widespread adoption of IoT is hampered by inherent vulnerabilities related to security, privacy, and the establishment of trust among devices and users. The decentralized and dynamic architecture of IoT networks, coupled with the resource constraints of many IoT devices, makes them particularly susceptible to various cyber threats, including data breaches, denial-of-service attacks, and unauthorized access [2].

Traditional security mechanisms often fall short in addressing the unique challenges posed by IoT environments. For instance, centralized trust management models suffer from single points of failure, scalability limitations, and increased vulnerability to attacks. Similarly, static access control policies struggle to adapt to the dynamic and context-aware nature of IoT device behavior [3].

Consequently, there is a pressing need for advanced security solutions that can intelligently manage trust and enforce robust access control in these complex ecosystems. Artificial Intelligence (AI) and cryptographic techniques have emerged as powerful tools to tackle these challenges. AI, with its capabilities in machine learning, anomaly detection, and predictive analytics, offers dynamic and adaptive solutions for identifying threats and assessing device trustworthiness [4]. Cryptography, on the other hand, provides fundamental security primitives such as encryption, digital signatures, and secure multi-party computation, which are essential for ensuring data privacy, integrity, and authentication [5]. The synergistic integration of AI and cryptography holds the promise of creating resilient and intelligent security frameworks for IoT systems.

*Corresponding author. Email: duhaalubady@gmail.com

This paper aims to provide a comprehensive and up-to-date review of AI-powered trust management and cryptographic access control in IoT systems. We will delve into the latest research and developments from the past three years (2023-2026), offering insights into the current state-of-the-art, identifying key challenges, and outlining future research directions. The structure of this paper is as follows: Section 2 provides an overview of traditional security approaches in IoT and their limitations. Section 3 explores various AI techniques for trust evaluation and their applications. Section 4 discusses different cryptographic methods and their integration with access control models. Section 5 examines hybrid models and the benefits of combining these two domains. Section 6 highlights new developments and technologies shaping the future of IoT security. Section 7 addresses the persistent hurdles and areas requiring further investigation. Finally, Section 8 summarizes the key findings and offers a final outlook.

2. BACKGROUND AND RELATED WORK

2.1 Traditional Trust Management in IoT

Traditional trust management in IoT often relies on centralized models where a trusted third party (TTP) or a central server is responsible for assessing and managing trust relationships [1]. These models suffer from single points of failure, scalability limitations, and increased vulnerability to attacks [6]. As the number of IoT devices rapidly increases, centralized systems struggle to handle the immense volume of data and interactions, leading to performance bottlenecks [7]. Recent research highlights that while traditional methods provide a foundational understanding, their static nature and susceptibility to single points of failure make them inadequate for the dynamic and decentralized nature of modern IoT ecosystems [8].

2.2 Traditional Access Control in IoT

Access control mechanisms are crucial for regulating which entities can perform specific actions on IoT devices and data. Traditional access control models, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), rely on predefined, static rules that struggle to adapt to the dynamic and context-aware nature of IoT environments [9]. This lack of adaptability makes them ineffective against evolving threats and insider attacks. The increasing complexity and heterogeneity of IoT devices necessitate more flexible and adaptive access control solutions that can respond to real-time changes and emerging threats [10].

2.3 Overview of AI in Cybersecurity

Artificial Intelligence has emerged as a transformative force in cybersecurity, offering advanced capabilities for threat detection, anomaly identification, and automated response. AI techniques, particularly machine learning and deep learning, can analyze vast amounts of data to identify patterns indicative of malicious behavior, often surpassing the capabilities of traditional rule-based systems [11]. In the context of IoT security, AI can be leveraged to identify unusual patterns in device behavior or network traffic that may signal a security breach. Recent studies emphasize AI's role in shifting from reactive defense to proactive risk management in OT/IoT environments, highlighting its potential for continuous learning and adaptation to new threats [12].

2.4 Overview of Cryptography in IoT

Cryptography forms the bedrock of secure communication and data protection in digital systems. In IoT, cryptographic techniques are essential for ensuring the confidentiality, integrity, and authenticity of data exchanged between devices and across networks . Key cryptographic primitives and their applications in IoT include encryption, which protects data from unauthorized access by transforming it into an unreadable format [13] . While these traditional approaches provide foundational security, the dynamic and complex nature of IoT necessitates more advanced and integrated solutions.Research continues to focus on enhancing IoT security with resource-efficient cryptography, including lightweight and hybrid cryptographic schemes tailored for constrained IoT environments [14].

3. AI-POWERED TRUST MANAGEMENT IN IOT SYSTEMS

AI-powered trust management in IoT systems involves leveraging artificial intelligence techniques to dynamically assess and maintain trust relationships among heterogeneous devices and entities . This approach moves beyond static, predefined trust models to create adaptive and intelligent systems capable of responding to evolving threats and behaviors.The integration of AI in trust management is crucial for addressing the inherent vulnerabilities of IoT ecosystems, providing a more resilient and intelligent security framework [15].

3.1 Definition and Principles of AI-Powered Trust

AI-powered trust management refers to the application of AI algorithms and models to collect, analyze, and interpret data related to the behavior, interactions, and context of IoT entities to infer and manage their trustworthiness. The principles underpinning this approach include dynamic trust assessment, where trust is not static but continuously updated based on

real-time observations and historical interactions [16]. This dynamic nature allows for continuous adaptation to new threats and behaviors, making it a robust solution for complex IoT environments [8], as shown in Fig.1.

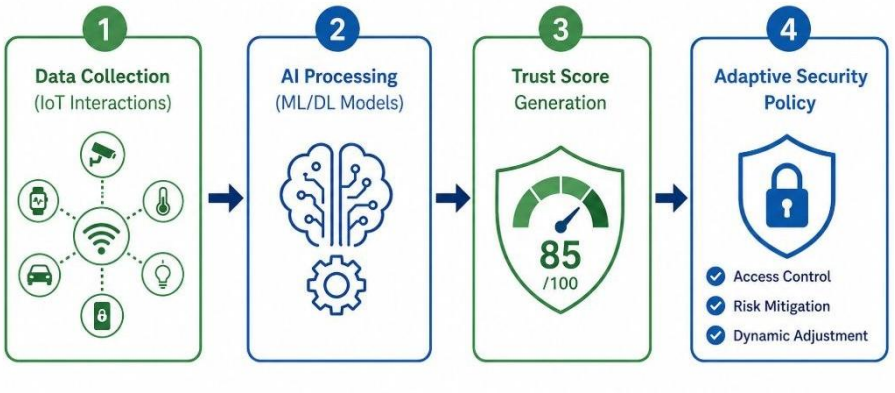

Fig. 1. AI - Powerd Trust process.

3.2 AI Techniques for Trust Evaluation

Various AI techniques are employed for trust evaluation in IoT systems, each offering distinct advantages . Machine Learning (ML) algorithms, such as Support Vector Machines (SVM), Decision Trees, and K-Nearest Neighbors (KNN), can be trained on historical data to classify devices as trustworthy or untrustworthy. Deep Learning (DL) networks, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are particularly effective in processing complex and high-dimensional data generated by IoT devices [17]. Federated Learning (FL) is a decentralized machine learning approach that allows multiple IoT devices to collaboratively train a shared model without exchanging their raw data [6]. Reinforcement Learning (RL) agents can learn optimal trust management policies through trial and error, adapting to dynamic IoT environments and making decisions that maximize overall system trust and security. Recent advancements also highlight the use of explainable AI (XAI) to provide transparency in trust decisions, which is crucial for critical IoT applications [9].

3.3 Applications and Benefits

AI-powered trust management offers several significant applications and benefits for IoT systems. AI models can effectively detect deviations from normal device behavior or network traffic patterns, signaling potential security breaches or malicious activities [6]. By continuously analyzing device interactions and data flows, AI can build comprehensive behavioral profiles for each IoT entity. This enables proactive threat detection and response, significantly enhancing the overall security posture of IoT deployments .Furthermore, AI can optimize resource allocation and improve the efficiency of trust assessment processes in large-scale IoT networks [18].

3.4 Challenges in AI-Powered Trust Management

Despite its advantages, AI-powered trust management faces several challenges. Deep learning models, while powerful, can be black boxes, making it difficult to understand why a particular trust decision was made. AI models can inherit biases from their training data, leading to unfair or discriminatory trust assessments. Although federated learning aids in decentralization, deploying complex AI models on resource-constrained IoT devices still poses challenges in terms of computational power, memory, and energy consumption. Other challenges include adversarial attacks on AI models, data quality issues, and the need for robust evaluation metrics that reflect real-world deployment scenarios [12], [13].

4. CRYPTOGRAPHIC ACCESS CONTROL IN IOT SYSTEMS

Cryptographic access control in IoT systems leverages cryptographic primitives to enforce secure access policies, ensuring that only authorized entities can interact with devices and data.This approach provides a robust layer of security by guaranteeing confidentiality, integrity, and authenticity, which are foundational for building trustworthy IoT environments. Unlike traditional access control mechanisms that that rely solely on permissions and roles, cryptographic methods embed security directly into the data and communication channels. This direct embedding of security at the data level makes cryptographic access control particularly effective in decentralized and dynamic IoT settings [19], As shown in Fig.2.

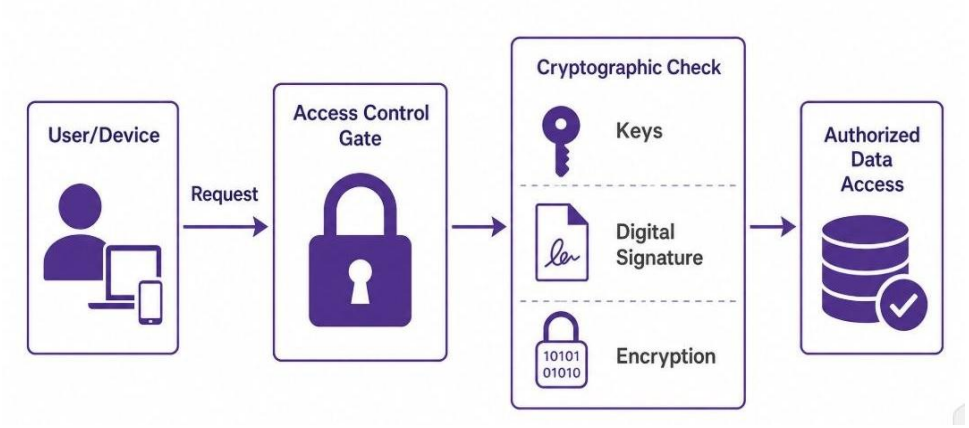

Fig. 2. Cryptographic access control.

4.1 Fundamentals of Cryptographic Access Control

Cryptographic access control is a cornerstone of robust security in IoT systems, employing various cryptographic primitives to establish and enforce secure access policies [1], [14]. This approach moves beyond mere authentication and authorization by embedding security directly into the data and communication channels, thereby ensuring that only legitimate entities can interact with sensitive resources [15]. The fundamental principles underpinning cryptographic access control include:

- **Confidentiality**: Paramount, ensuring that information remains private and is accessible exclusively to authorized parties. This is primarily achieved through encryption, where data is transformed into an unreadable format, rendering it unintelligible to unauthorized interceptors, [16]. In IoT, this is essential for protecting sensitive data transmitted by devices, such as patient information in healthcare or operational data in industrial automation.
- **Integrity**: Ensures that data has not been tampered with or modified without authorization. This is achieved through hashing and digital signatures, which provide a mechanism to verify that data is authentic and has not been altered during transmission or storage [15].
- **Authentication**: Verifies the identity of devices and users involved in interactions. Strong authentication mechanisms ensure that entities attempting to access IoT resources are indeed who they claim to be, preventing impersonation and unauthorized access [16].
- **Non-repudiation**: Guarantees that a party cannot deny their involvement in a particular transaction or action. This is typically achieved through digital signatures, which provide undeniable proof of data origin and integrity [17].

These principles are critical for establishing a secure and trustworthy environment in IoT, especially given the increasing number of interconnected devices and the sensitive nature of the data they handle [18].

4.2 Cryptographic Techniques for Access Control

A variety of cryptographic techniques are used to implement access control in IoT systems, considering resource constraints and security requirements:

- **Symmetric-key Cryptography**: Uses a single key for both encryption and decryption. It is computationally efficient and suitable for resource-constrained IoT devices. As shown in Fig.3 Examples include AES (Advanced Encryption Standard) [19]. However, a major challenge lies in the secure management and distribution of keys among numerous devices.

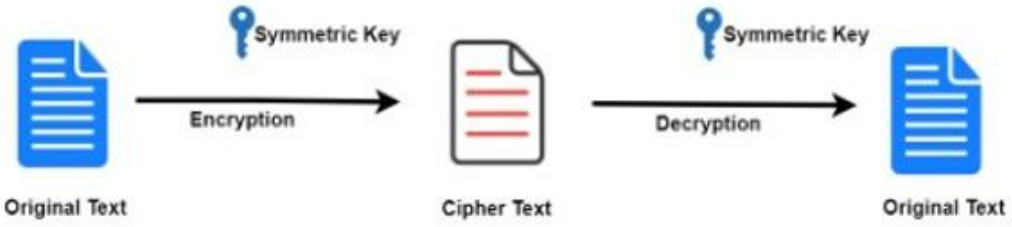

Fig. 3. Symmetric key Cryptography.

- **Asymmetric-key Cryptography (Public-key Cryptography):** Uses a pair of keys (a public key and a private key). In Fig.4 the public key is available to everyone for encryption, while the private key is kept secret for decryption. This approach provides robust solutions for authentication and digital key exchange, such as RSA and Elliptic Curve Cryptography (ECC) [1]. ECC is often preferred in IoT due to its resource efficiency while providing a high level of security [20].

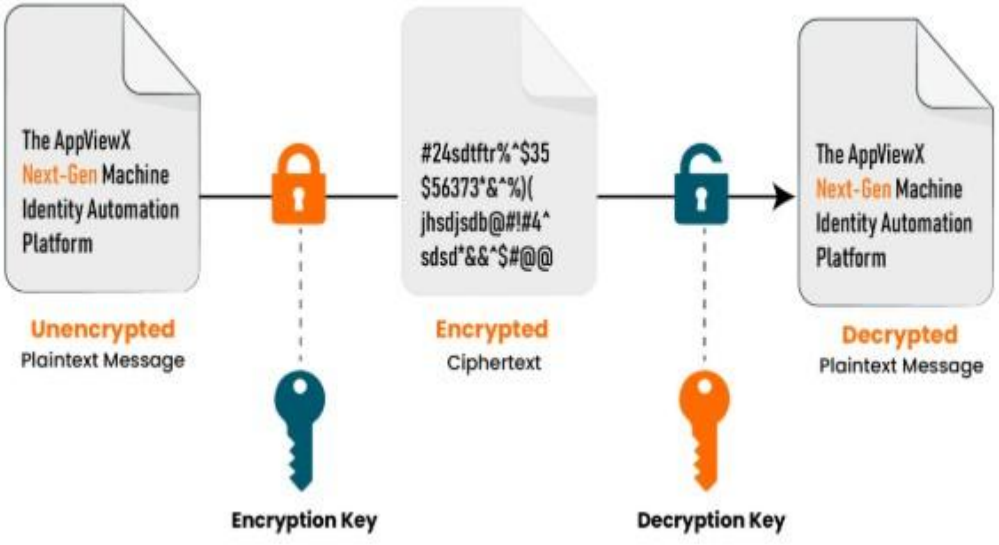

Fig. 4. Asymmetric key Cryptography

- **Digital Signatures**: Used to ensure the authenticity and integrity of messages and data. A signature is created using the sender's private key and can be verified using the sender's public key, ensuring that the data has not been tampered with and originates from a legitimate source [18].
- **Hash Functions**: Generate unique, fixed-size outputs from input data. They are used for data integrity checks and secure password storage.
- **Key Management**: Involves the secure generation, distribution, storage, and revocation of cryptographic keys. This presents a significant challenge in large-scale IoT deployments, requiring robust and efficient solutions. Recent research explores blockchain-enabled identity management for IoT to address key management challenges and enhance security against adversarial AI [17].

4.3 Challenges of Cryptographic Access Control in IoT

Despite its effectiveness, cryptographic access control in IoT faces unique challenges:

- **Resource Constraints**: Many IoT devices have limited processing power, memory, and energy, making the implementation of complex cryptographic algorithms challenging. Lightweight Cryptography (LWC) solutions that balance security and efficiency are required [20].
- **Scalability**: As the number of IoT devices grows, managing keys and access policies for a vast number of devices becomes increasingly complex [21].
- **Interoperability**: The diversity in IoT devices and protocols makes it difficult to establish a unified and interoperable access control framework [2].
- **Quantum Threats**: Advances in quantum computing threaten to break traditional cryptographic algorithms, necessitating a transition to Post-Quantum Cryptography (PQC) [3]. However, PQC comes with its own challenges in terms of larger key sizes and computational requirements [18].

Addressing these challenges requires the development of innovative cryptographic solutions that adapt to the dynamic and resource-constrained nature of IoT environments, while providing robust security against current and future threats [19].

5. HYBRID MODELS AND THE BENEFITS OF COMBINING THESE TWO DOMAINS

Hybrid models that combine AI and cryptographic techniques show immense potential in enhancing the security of IoT systems. This synergistic integration aims to overcome the individual limitations of each approach, leading to more robust and flexible solutions. For instance, AI can provide dynamic and adaptive trust management, while cryptography ensures confidentiality, integrity, and authentication at the data level [19]. The convergence of AI and cryptography offers a powerful paradigm for creating resilient and intelligent security frameworks for IoT systems, addressing the limitations of relying solely on one approach [6].

Key benefits of hybrid models include:

1. **Enhanced Security**: AI can identify anomalous patterns and emerging threats that traditional cryptographic mechanisms might fail to detect, while cryptography provides fundamental protection against unauthorized access and data manipulation. This layered approach creates a more comprehensive defense against sophisticated cyberattacks [1].
2. **Adaptive Trust**: AI-driven trust management allows for continuous assessment and adaptation of trust levels based on real-time behavior and context, making the system more responsive to dynamic threats. Cryptography then secures the communication and data exchanges based on these dynamically established trust relationships [8].
3. **Improved Efficiency**: By leveraging AI for intelligent decision-making and anomaly detection, the computational overhead of cryptographic operations can be optimized. For example, AI can prioritize which data needs stronger encryption or identify less critical data that can use lightweight cryptographic methods, thus balancing security with resource constraints [9].
4. **Privacy Preservation**: Techniques like federated learning, combined with homomorphic encryption, allow AI models to be trained on sensitive data without compromising privacy. This ensures that valuable insights can be extracted from distributed IoT data while maintaining strict confidentiality [10].
5. **Scalability and Interoperability**: Hybrid models can be designed to scale with the growing number of IoT devices and to operate across diverse platforms and protocols. AI can help manage the complexity of large-scale deployments, while cryptographic standards ensure secure communication between heterogeneous devices [11].

These benefits underscore the importance of integrating AI and cryptographic techniques to build future-proof security solutions for the evolving IoT landscape as shown in fig.5. Research in this area is rapidly advancing, with a focus on developing practical and deployable hybrid frameworks [12].

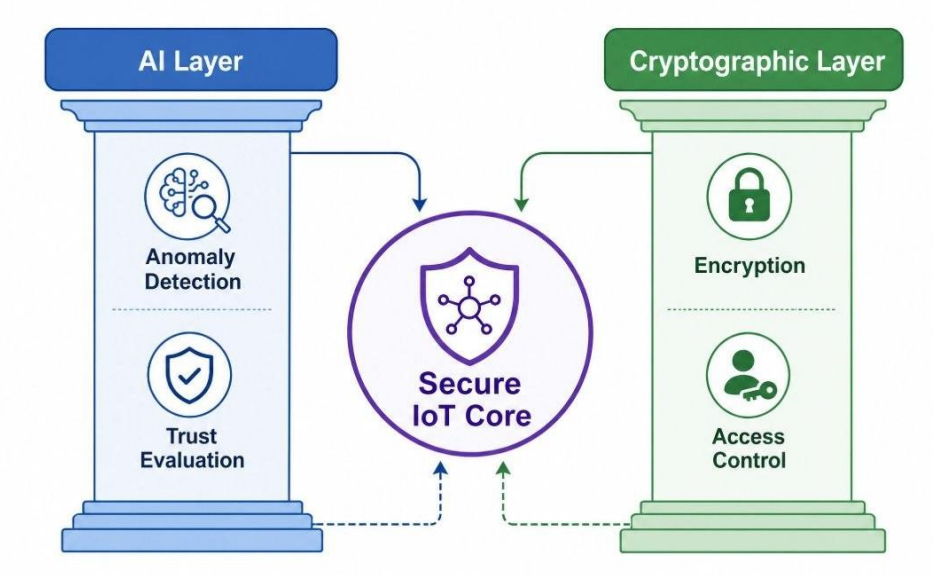

Fig. 5. Hybrid Models AI and Cryptographic

6. EMERGING TRENDS AND FUTURE DIRECTIONS

The landscape of AI-powered trust management and cryptographic access control in IoT is continuously evolving, driven by advancements in both fields. Several emerging trends and future directions are poised to shape the next generation of secure IoT systems:

1. **Blockchain and Distributed Ledger Technologies (DLT)** for Trust: Blockchain and DLTs are increasingly being explored for decentralized trust management in IoT. They offer immutable records, transparency, and enhanced security, which can complement
2. **AI-driven trust models** by providing a robust foundation for identity and access management [6]. The integration of blockchain with AI can create self-sovereign identity solutions and more resilient trust frameworks [17].
3. **Post-Quantum Cryptography (PQC):** With the advent of quantum computing, traditional cryptographic algorithms are at risk. The development and deployment of PQC are critical for ensuring long-term security in IoT systems. Research is focused on designing lightweight PQC algorithms that can operate efficiently on resource-constrained IoT devices [18].
4. **Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMC):** These advanced cryptographic techniques allow computations on encrypted data, enabling privacy-preserving AI in IoT. HE and SMC can facilitate collaborative AI model training and data analysis without exposing sensitive information, addressing key privacy concerns in federated learning scenarios [10].
5. **Explainable AI (XAI) for Trust and Security**: As AI models become more complex, understanding their decision-making processes is crucial, especially in security-critical applications. XAI aims to make AI models more transparent and interpretable, which can enhance trust in AI-powered security systems and aid in debugging and auditing [2].
6. **Edge AI and TinyML for On-Device Security**: Pushing AI capabilities to the edge and directly onto IoT devices (TinyML) can enable real-time threat detection and response, reducing latency and reliance on cloud infrastructure. This trend is vital for autonomous IoT systems where immediate decision-making is paramount [9].
7. **AI for Automated Vulnerability Detection and Patching**: AI can be used to automatically identify vulnerabilities in IoT device firmware and software, and even suggest or generate patches. This can significantly reduce the time to respond to new threats and improve the overall security posture of IoT ecosystems [12].

These trends indicate a move towards more autonomous, intelligent, and privacy-preserving security solutions that can adapt to the dynamic and challenging environment of IoT [3], [9].

7. PERSISTENT CHALLENGES AND FUTURE RESEARCH AVENUES

Despite significant advancements, several persistent challenges remain in the realm of AI-powered trust management and cryptographic access control in IoT, opening up numerous avenues for future research: [1], [7]

1. **Scalability and Resource Constraints:** Balancing robust security with the limited computational, memory, and energy resources of many IoT devices remains a fundamental challenge. Future research needs to focus on developing ultra-lightweight AI algorithms and cryptographic primitives that can deliver high security with minimal overhead [5].
2. **Interoperability and Standardization**: The highly fragmented nature of the IoT ecosystem, with diverse devices, protocols, and platforms, hinders the development of unified security solutions. Establishing interoperable standards for AI-powered trust and cryptographic access control is crucial for widespread adoption and seamless integration [11].
3. **Data Quality and Bias in AI Models**: The effectiveness of AI-powered security solutions heavily relies on the quality and representativeness of training data. Addressing issues of data scarcity, data poisoning attacks, and algorithmic bias is essential to ensure fair and reliable trust assessments [7].
4. **Adversarial AI and Robustness**: AI models themselves are vulnerable to adversarial attacks, where subtle perturbations to input data can lead to incorrect classifications or decisions. Developing AI models that are robust against such attacks is a critical area of research for maintaining the integrity of AI-powered security systems [13].
5. **Ethical and Legal Considerations**: The use of AI for trust management raises ethical concerns regarding privacy, surveillance, and algorithmic accountability. Future research must address these ethical implications and work towards establishing clear legal and regulatory frameworks for AI-powered IoT security [20].
6. **Dynamic Threat Landscape**: The nature of cyber threats is constantly evolving. Security solutions must be dynamic and adaptive enough to counter new and sophisticated attack vectors. Research into proactive and predictive security mechanisms, leveraging advanced AI techniques, is vital [3].
7. **Human-in-the-Loop Security**: While automation is key, human oversight and intervention remain crucial. Future systems should incorporate effective human-in-the-loop mechanisms to allow security analysts to understand, validate, and override AI decisions when necessary, enhancing overall system reliability and trust [21].

Addressing these challenges will require interdisciplinary collaboration between AI researchers, cryptographers, security engineers, and policymakers to develop comprehensive and sustainable solutions for secure IoT ecosystems [5], [20].

8. CONCLUSION

The convergence of AI and cryptography offers a promising pathway to address the complex security, privacy, and trust challenges inherent in the rapidly expanding Internet of Things ecosystem. This paper has provided a comprehensive review of AI-powered trust management and cryptographic access control mechanisms, highlighting their fundamental principles, advanced techniques, and synergistic integration. We have explored how AI, through machine learning, deep learning, and federated learning, can enable dynamic trust assessment, anomaly detection, and adaptive security policies. Concurrently, cryptographic techniques such as symmetric and asymmetric encryption, digital signatures, and secure multi-party computation provide foundational guarantees for data confidentiality, integrity, and authenticity. The benefits of combining these two domains in hybrid models are evident in enhanced security, adaptive trust, improved efficiency, and privacy preservation. While significant progress has been made, persistent challenges related to scalability, resource constraints, interoperability, data quality, adversarial AI, and ethical considerations continue to drive future research. Emerging trends such as blockchain for trust, post-quantum cryptography, homomorphic encryption, and explainable AI are shaping the future of secure IoT. By fostering interdisciplinary research and development, the IoT community can build more robust, adaptive, and context-aware security frameworks, paving the way for a truly trustworthy and resilient interconnected world.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Funding

The authors declare that this research received no external funding.

Acknowledgment

The authors would like to express their sincere gratitude to everyone who contributed to the successful completion of this research through their valuable support, encouragement, and constructive suggestions. Special appreciation is extended to the Babylonian Journal of Internet of Things for its continuous academic support and for providing a stimulating research environment that greatly facilitated this work.

References

[1] F. C. Ogenyi, C. N. Ugwu, and O. P.-C. Ugwu, "Securing the future: AI-driven cybersecurity in the age of autonomous IoT," *Frontiers in Internet of Things*, vol. 4, Art. no. 1658273, 2025, doi: 10.3389/friot.2025.1658273.

[2] Q. Xue, P. Xue, Z. Wang, and H. Ma, "Artificial intelligence for cybersecurity in IoT-edge systems: A structured review of methods, datasets, evaluation, and deployment challenges," *Electronics*, vol. 15, no. 11, Art. no. 2409, 2026, doi: 10.3390/electronics15112409.

[3] Nozomi Networks, "In 2026, AI-powered cybersecurity for OT & IoT is table stakes," Feb. 11, 2026. [Online]. Available: https://www.nozominetworks.com/blog/in-2026-ai-powered-cybersecurity-for-ot-iot-is-table-stakes

[4] Nozomi Networks, "Securing the unseen: AI-driven OT/IoT risk management," Apr. 18, 2025. [Online]. Available: https://www.nozominetworks.com/resources/securing-the-unseen-ai-driven-ot-iot-risk-management

[5] Z. A. Haider, A. Zeb, A. M. Islam, T. Rahman, A. Arishi, and I. Ullah, "Enhancing IoT security with resource-efficient cryptography: A comprehensive review of lightweight and hybrid algorithms," *Computer Science Review*, vol. 59, Art. no. 100861, 2026, doi: 10.1016/j.cosrev.2025.100861.

[6] M. Alharbi, K. Haseeb, N. Z. Jhanjhi, A. Khan, M. Humayun, and M. A. Khan, "Blockchain-driven trust management and AI computing for sensor networks optimization," *Scientific Reports*, vol. 16, Art. no. 41302, 2026, doi: 10.1038/s41598-026-41302-y.

[7] G. D'Aniello and L. Fotia, "Blockchain and AI-based methods for trust management in IoT: A comprehensive survey," *Internet of Things*, vol. 34, Art. no. 101755, 2025, doi: 10.1016/j.iot.2025.101755.

[8] International Telecommunication Union (ITU), "Designing the trust management for agentic AI," *AI for Good Global Summit 2026 Workshop*, Jul. 9, 2026. [Online]. Available: https://aiforgood.itu.int/event/designing-the-trust-management-for-agentic-ai

[9] Z. Zhang, "A review of embedded artificial intelligence research (2023-2026): Technological advancements, representative advances, and future prospects," *Micromachines*, vol. 17, no. 5, Art. no. 586, 2026, doi: 10.3390/mi17050586.

[10] S. Dhole, "Dominate IoT data privacy: Strong safeguards for connected devices in 2026," TrustCloud, 2026. [Online]. Available: https://trustcloud.ai/privacy/dominate-iot-data-privacy-strong-safeguards-for-connected-devices-in-2026

[11] Renesas Electronics Corp., "IoT security solutions: Secure connected devices." [Online]. Available: https://www.renesas.com/en/key-technologies/security/iot-security

[12] M. N. Halgamuge and D. Niyato, "Adaptive edge security framework for dynamic IoT security policies in diverse environments," *Computers & Security*, vol. 150, Art. no. 104190, 2025, doi: 10.1016/j.cose.2024.104190.

[13] Q. Chen, L. Tan, J. Tang, and X. Qu, "AI-enabled IoT security: A survey on advances, challenges, and cross-domain collaborative frameworks," in *Proc. 8th Int. Conf. Computer Information Science and Artificial Intelligence (CISAI)*, 2025, doi: 10.1145/3773365.3773619.

[14] T. Hidayat and I. Rusydi, "The role of cryptography in data security for the Internet of Things (IoT)," *Interdisciplinary Journal of Global Multidisciplinary*, vol. 2, no. 1, pp. 763-773, 2026.

[15] K. Mariappan, P. Ganesan, and S. K. Jagatheesaperumal, "IoT access control and authentication schemes," in *Internet of Things Security: Attacks, Tools, Techniques and Challenges*, P. Mishra, S. K. Jagatheesaperumal, A. Kumar, and B. B. Gupta, Eds. Amsterdam, The Netherlands: Elsevier, 2025, pp. 87-106, doi: 10.1016/B978-0-44-333759-8.00013-7.

[16] F. Thabit, Ö. Can, A. O. Aljahdali, G. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing IoT security," *Internet of Things*, vol. 22, Art. no. 100759, 2023, doi: 10.1016/j.iot.2023.100759.

[17] management for IoT: A multi-layered defense against adversarial AI," Sci. Rep., vol. 16, Art. no. 35208, 2026, doi: 10.1038/s41598-026-35208-y.

[18] M. M. H. Emon, M. Mazid-Ul-Haque, M. S. A. Chowdhury, and K. M. Rahman, "Fortifying smart city applications: Cryptographic security in e-health, e-commerce, e-banking, and e-governance," in Securing Smart Cities Through Modern

Cryptography Technologies, M. Al-Zubaidie, Ed. Hershey, PA, USA: IGI Global Scientific Publishing, 2026, pp. 1-42, doi: 10.4018/979-8-3373-3326-7.ch001.
[19] M. S. Sumathi, J. Shruthi, V. Jain, G. K. Kumar, and Z. Z. Khan, "Using artificial intelligence (AI) and Internet of Things (IoT) for improving network security by hybrid cryptography approach," Evergreen, vol. 10, no. 2, pp. 1133-1139, 2023, doi: 10.5109/6793674.
[20] L. C. Kelepile and N. P.-I. G. Eiaseb, "Navigating the ethics of big data: Responsible AI and data governance in IoT-powered marketing," in IoT-Driven Business Transformation: Strategy, Data, Trust, and Security, J. P. Nautwima and A. R. Asa, Eds. Hershey, PA, USA: IGI Global Scientific Publishing, 2026, pp. 283-308, doi: 10.4018/979-8-2600-1263-5.ch010.
[21] A. Singh, N. Singh, O. Singh, and R. Vinoth, "AI-powered smart grids: Security challenges and intelligent energy management approaches," International Journal of Communication Networks and Information Security, vol. 18, no. 1, pp. 37-53, 2026.