AI data revolution: without cryptography, where does true intelligence come from?

January 19, 2026

We are speeding towards a future driven by AI agents, from daily office work and life planning to more complex tasks like autonomous vehicle path planning, medical AI image analysis, financial model risk assessment, and intelligent manufacturing quality control etc., the reach of intelligent decision-making is extending to every key area of the socio-economic landscape. However, in this frenzied race measured by the complexity of AI algorithms and the scale of computing power, a more fundamental question has been severely neglected: Is the foundation of this intelligent behemoth we've poured all our resources into building — the data we're "feeding" the AI — authentic and reliable? If the source of the "data fuel" driving all intelligence is questionable and untrustworthy, will we ultimately obtain a temple of wisdom leading to the future, or a precarious building built on quicksand, ready to collapse at any moment?

The root of the problem lies in a near-paradoxical vulnerability in the current AI paradigm: AI agents exhibit increasingly powerful "thinking" abilities, but their "cognition" is based on unconditional and blind trust in input data. AI lacks the innate human instinct for questioning and tracing, leading us to tolerate the fatal flaw of data reliability while pursuing advanced intelligence. In the open, complex, and adversarial real world, this "garbage in, garbage out" logic is tantamount to feeding an ignorant child a bunch of erroneous viewpoints, this child will inevitably make wrong decisions, with consequences far exceeding a few percentage points decrease in model accuracy.

1. From intelligent driving to life and health: a microcosm of a systemic trust crisis

Taking autonomous driving as an example, we can get a glimpse into the problem. If an autonomous vehicle cannot verify the true source of its perception data (whether it comes from trusted sensors?), its timeliness (whether the high-precision map has been updated?), and its transmission security (whether the commands have been tampered with en route?), it may make catastrophic misjudgments at critical moments. Outdated or falsified data is absolute "fact" to AI, and its "intelligent" decisions will at best fail, and at worst be fatal.

This logic holds true worldwide: in the medical field, if medical imaging data used to assist diagnosis is maliciously contaminated or mislabeled, the "benign" judgment given by AI may delay treatment; in the financial field, if the identity and time of transaction data used for risk assessment are unclear, the model may condone fraud or wrongly penalize legitimate companies; in industrial manufacturing, if the readings of sensors on the production line cannot be reliably traced and verified, the so-called "intelligent quality inspection" will lose all its quality foundation. This reveals a harsh truth: on the journey to building trustworthy AI, any single, isolated "security measure" is like a pearl with a broken string, unable to form an effective defense. AI faces a systemic trust crisis that permeates data identity, data timeliness, data transmission, and future security.

2. Building the cornerstone of ai data trust: a four-in-one trusted cryptographic application system

We must launch a fundamental revolution in data "feeding". The cornerstone of this revolution is no longer a single, cool, isolated AI model or algorithm, but a systematic, trusted cryptographic application system that spans the entire lifecycle of data, from its "birth" to its "consumption." This system is like establishing an unforgeable "legal, notarized, circulation, and future security" for the data world. It consists of four indispensable pillars working together:

(1) **The first pillar: HTTPS encryption** — the "bulletproof armored truck" and "secret channel" for data.

HTTPS encryption ensures the secure transmission of data during its long network journey. When a client and server establish a connection, a session key known only to both parties is negotiated through a key exchange algorithm. Subsequently, all data is transmitted using this key in encryption. This achieves: 1) Confidentiality: Even if the data is intercepted, it cannot be decrypted and read. 2) Integrity: The built-in message authentication mechanism can detect any tampering during transmission. It perfectly guarantees the security of data "on the way" and serves as a secure bridge connecting trusted data sources and trusted AI.

(2) **The second pillar: digital signature** — the “ID card” and “Seal” for data.

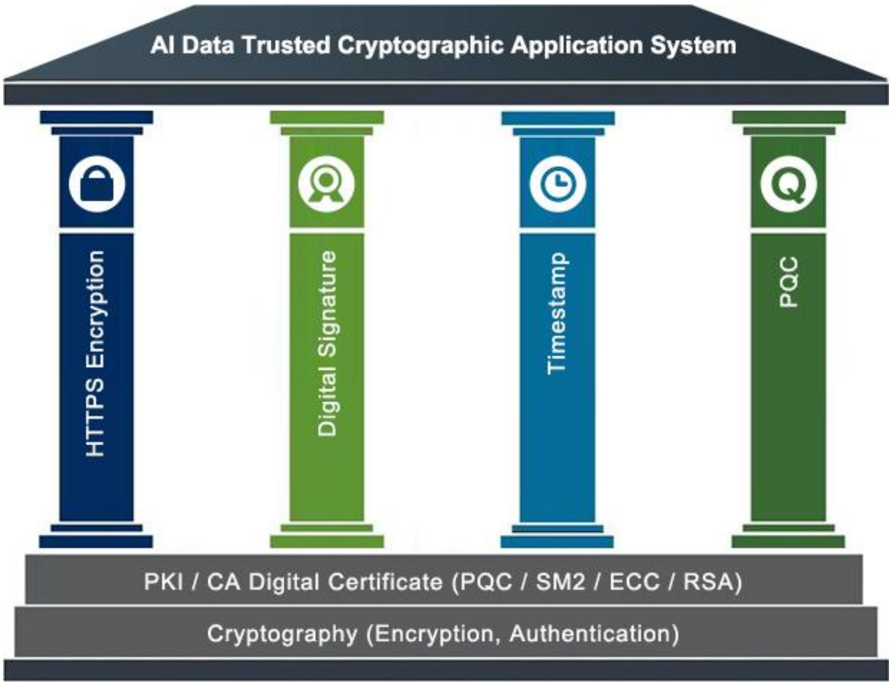
Digital signatures serve far more than just "encryption." Based on Public Key Infrastructure (PKI), data producers use their private keys to generate a unique "signature" on their data. Any recipient can verify this signature using the publicly available public key. If the verification is successful, it proves with absolute certainty that: 1) the data source is trustworthy: the data was indeed created by the holder of the private key (the producer). 2) the data is intact: not even a single bit of the data has been tampered with since it was signed. This fundamentally solves the problems of identity fraud and content tampering, and provides irrefutable electronic evidence for subsequent auditing and accountability.

(3) **The third pillar: timestamp** — the “official birth certificate” and “time notarization” of data.

Timestamp is provided by a trusted timestamp service (TSA). The process involves sending the HASH value (digital fingerprint) of the data to the TSA. The TSA receives the HASH and signs it along with its authoritative time (e.g., UTC time), generating a timestamp signature. This authoritatively proves that the data existed at "that" point in time. AI systems can easily determine whether data is within a valid time window, automatically filtering out expired information and preventing decision-making errors caused by outdated data. Timestamps also provide reliable proof of when data was used.

(4) **The fourth pillar: PQC** — a future-proof “quantum-resistant security lock”.

This is a forward-looking strategy to address "Q-Day" (the day a quantum computer breaks existing cryptographic algorithms). Post-quantum cryptography (PQC) designs new algorithms based on mathematical problems that quantum computers struggle to solve (such as lattice problems and multivariable equations). NIST are accelerating the standardization of PQC. Using it for digital signatures and key exchange means that the data credentials we generate today for smart cars, medical records, financial contracts, and other applications, as well as their transmission and circulation, will still be able to withstand the most powerful computational attacks for decades to come, ensuring the long-term preservation of trust.


AI Data Trusted Cryptographic Application System
HTTPS Encryption
Digital Signature
Timestamp
PQC
PKI / CA Digital Certificate (PQC / SM2 / ECC / RSA)
Cryptography (Encryption, Authentication)

The above four pillars are not simply stacked together, but organically integrated, transforming data from raw, anonymous, perishable, and vulnerable "raw materials" into "standard intelligent nutrients" that are clearly identified, time-definite, securely transmitted (anti-tampering and anti-theft), and reliable for the future. This is a revolution in AI 'feeding', it is the key for AI to truly become safe and usable, and it is the winning strategy for AI agents.

3. Redefining AI-friendly data: from format-friendly to trust-friendly

Based on this systematic understanding, we must fundamentally reshape the definition of "AI-friendly data." It can no longer remain at the rudimentary stage of "well-formatted, clearly labeled, and easy for models to read." Truly AI-friendly data, addressing serious real-world challenges, should be defined by a multiplier effect model:

Truly AI-friendly data = Structured machine-readable × Trusted cryptographic applications (trusted identity × trusted time × trusted transmission × trusted future)

The "multiplication sign" here means that if any one of the trust dimensions is missing (with a value of zero), the total trust value of the entire data will be zero, no matter how strong the other dimensions are. Only when all dimensions are satisfied simultaneously can the data release its full value, and only then can the AI agent generate trusted and reliable results.

When this model becomes an industry consensus and practice, it will bring about fundamental changes to the AI ecosystem:

(1) **Security model evolution**: from a passive, reactive approach of "vulnerability discovery - emergency patching" to "system immunity". Trusted cryptographic systems build proactive verification and filtering barriers at the data entry point.

(2) **Clearer definition of responsibility**: Moving from a "gray area" that is difficult to clarify after an accident to a process that is "auditable and traceable" throughout. Based on digital signatures and timestamps, any output can be traced back to the source and status of its input data.

(3) **Industry collaboration becomes possible**: fundamentally breaking down "data silos". When all participants follow a unified and trusted cryptographic standard, cross-institutional and cross-industry data sharing and joint modeling will be conducted securely within a pre-defined trust framework, fostering a more robust and trusted ecosystem.

4. Trusted cryptography applications are the "value anchor" in the AI era

In conclusion, AI data "feeding" urgently needs a revolution in trusted cryptographic applications: systematic applications of trusted cryptographic must transform from an "optional" in AI projects to a "must-have" in the development of the intelligent era, serving as the "anchor" for realizing the value of AI.

Without trusted cryptographic applications as a foundation, the data fed to AI will forever be "garbage data" of dubious origin, unclear timeliness, and questionable path. On the basis of such rampant garbage data, no matter how sophisticated the AI algorithm, the "intelligence" it generates will inevitably be unstable, logically distorted, and fraught with danger, incapable of fulfilling critical missions. Such AI is not a partner, but a burden; not progress, but regression.

Therefore, the author urges the entire AI, cryptography, and cybersecurity industries to take immediate action to elevate the construction and integration of trusted cryptographic application systems to a strategic core position within AI infrastructure. This requires collaboration among algorithm scientists, cryptographers, cybersecurity engineers, software and hardware engineers, standard setters, and policy regulators.

Without trusted cryptographic applications, there are no trusted data sources; without trusted data sources, where does truly trustworthy artificial intelligence come from? Only on this solid, transparent, and future-oriented foundation of trust that cryptography has jointly forged for us can AI agents completely escape the predicament of being "advanced followers" and truly evolve into reliable intelligent partners that can co-evolve with human civilization and be fully entrusted with our lives.
This is not just a choice of technological path, but also the most fundamental ethical and safety responsibility that we, as AI creators, must fulfill in this intelligent era.

Richard Wang

January 19, 2026
In Shenzhen, China

Follow ZT Browser at X (Twitter) for more info.
The author has published 115 articles in English (more than 157K words)
and 258 articles in Chinese (more than 755K characters in total).