Future of cyberspace
A critical review of standard security protocols in the post-quantum era

Taleby Ahvanooey, Milad; Mazurczyk, Wojciech; Zhao, Jun; Caviglione, Luca; Choo, Kim Kwang Raymond; Kilger, Max; Conti, Mauro; Misoczki, Rafael

DOI
10.1016/j.cosrev.2025.100738

Publication date
2025

Document Version
Final published version

Published in
Computer Science Review

Contents lists available at ScienceDirect

Computer Science Review

journal homepage: www.elsevier.com/locate/cosrev

Review article

Future of cyberspace: A critical review of standard security protocols in the post-quantum era

Milad Taleby Ahvanooey [a,b,*], Wojciech Mazurczyk [a], Jun Zhao [b], Luca Caviglione [c], Kim-Kwang Raymond Choo [d], Max Kilger [d], Mauro Conti [e,f], Rafael Misoczki [g]

[a] Faculty of Electronics and Information Technology, Warsaw University of Technology, 00-665 Nowowiejska, Warszawa, Poland
[b] College of Computing and Data Science, Nanyang Technological University, P.O.Box. 639798, Singapore
[c] National Research Council of Italy (CNR), Via de Marini, 16149, Genoa, Italy
[d] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249-0631, USA
[e] Department of Mathematics, University of Padua, 63-35121, Padua, Italy
[f] Faculty of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, 2600 AA, Delft, Netherlands
[g] Cryptography Team, Meta, Menlo Park, CA 94025, USA

ARTICLE INFO

Keywords:
E-governance policies
Standard security protocols
Post-quantum cryptography
IoE security
Practical policy enforcement

ABSTRACT

Over the past three decades, standardizing organizations (e.g., the National Institute of Standards and Technology and Internet Engineering Task Force) have investigated the efficiency of cryptographic algorithms and provided (technical) guidelines for practitioners. For example, the (Datagram) Transport Layer Security "(D)TLS" 1.2/1.3 was designed to help industries implement and integrate such methods through underpinning infrastructures of Internet of Everything (IoE) environments with efficiency and efficacy in mind. The main goal underpinning such protocols is to protect the Internet connections between IoE machines from malicious activities such as unauthorized eavesdropping, monitoring, and tampering with messages. In theory, these protocols are supposed to be secure. Still, most existing implementations partially follow the standard features of (D)TLS 1.2/3, leaving them vulnerable to risks such as side-channel and network attacks. In this paper, we critically review the standard protocols deployed for the security management of data and connected machines, and also examine the recently discovered vulnerabilities that lead to successful zero-day attacks in IoE environments. Then, we discuss various potential countermeasures in the form of organizational policy enforcement strategies and mitigation approaches that can be used by cybersecurity practitioners, decision- and policy-makers. Finally, we identify both proactive and reactive solutions for further consideration and study, as well as propose alternative mechanisms and e-governance policies for standardizing organizations and engineers in future solution designs.

Contents

1. Introduction 2
2. Background on standard security protocols 3
2.1. Types of authentication schemes 3
2.1.1. U2D authentication 3
2.1.2. D2D authentication 4
2.2. Cyberattacks on IoE-based systems 5
3. Implementation challenges of standard security protocols 6
4. Update problems of in-use IoE machines 8
5. Post-quantum cryptography uncertainties 9
6. Unprecedented risks of cyberspace 10
6.1. Socio-economic and technological risks 10

* Corresponding author at: Faculty of Electronics and Information Technology, Warsaw University of Technology, 00-665 Nowowiejska, Warszawa, Poland.
E-mail addresses: M.taleby@ieee.org (M. Taleby Ahvanooey), wojciech.mazurczyk@pw.edu.pl (W. Mazurczyk), junzhao@ntu.edu.sg (J. Zhao), luca.caviglione@ge.imati.cnr.it (L. Caviglione), raymond.choo@fulbrightmail.org (K.-K.R. Choo), Max.Kilger@utsa.edu (M. Kilger), mauro.conti@unipd.it (M. Conti), rafam@meta.com (R. Misoczki).

https://doi.org/10.1016/j.cosrev.2025.100738
Received 10 February 2024; Received in revised form 14 February 2025; Accepted 17 February 2025
Available online 18 March 2025

6.2. Environmental risks ... 12
6.3. Cyberpsychological risks ... 12
7. Recommendations and future works ... 13
7.1. Strategic recommendations ... 13
7.2. Limitations and future works ... 14
8. Conclusion ... 15
CRediT authorship contribution statement ... 15
Declaration of competing interest ... 15
Acknowledgments ... 15
Data availability ... 15
References ... 15

1. Introduction

Shifting from Web 2.0 to Web 3.0 requires integrating more complex computing, ubiquitous, and intelligent infrastructures with the Internet [1]. Web 3.0 is the next generation of the World Wide Web ecosystem, which leverages Generative Artificial Intelligence (GenAI), decentralization, quantum computing, blockchain technologies, token-based economics, and many other technologies to increase consumer usefulness and openness [2]. Such a paradigm is designed to be independent by leveraging the distributed networks of smart gadgets rather than relying on centralized servers. In other words, the ultimate idea of the Web 3.0 ecosystem is to provide independent privacy control to users or communities over their information and financial assets when they interact in cyberspace [3]. Although this new iteration is still in the early stages of the public campaign development process, companies must consider advancing their underpinning infrastructures to provide the safe, competitive, and productive advantage of modern marketing as an approach to new digital economies [4]. As Web 3.0 matures, more enterprises are expected to upgrade, integrate, and/or implement Web 3.0 use cases on their platforms to increase the value of their businesses [5].

Data security and privacy remain two key considerations for the Internet of Everything (IoE) ecosystem in the post-quantum era [6]. Authentication schemes are commonly used to facilitate IoE security management [7], but they are insufficient measures on their own. In fact, the IoE is the conceptual network of connections between smart things, people, data, and processes to support intelligent decision-making and enhance user experiences via the Internet [6], which enables the connected cyberspace, where data is processed in a distributed manner. In such systems, Internet usage is generally not limited to smartphones, computers, and tablets, as anything (e.g., wearable or embedded devices) can be equipped with digital attributes and linked to other machines, processes, and people to produce intelligent services, exchange information, and improve compatible decision-making through the IoE network. Numerous IoE machines are connected to form the IoE architecture, where hardware and software-based security protocols can partially defeat cyberattacks. For instance, recent vulnerability analysis reports stated that cloud providers and computer manufacturers (e.g., Intel and AMD) have utilized many microcode and software security updates to protect against transient execution cyberattacks [8,9]. Such threats may take advantage of covert channels to discover vulnerabilities in the hardware device (e.g., millions of Intel/AMD CPUs were proven to be susceptible) that allow intruders to capture data across security boundaries (e.g., passwords and encryption keys) [10]. There is an ongoing race to design effective and efficient security protocols that are supposed to be resilient to unprecedented attacks crafted on classical or quantum computer security flaws [11]. In the literature, the state-of-the-art security algorithms exploit standard digital signatures, classical cryptosystems, or quantum-resistant protocols known as Post-Quantum Cryptography (PQC) [12]. However, they are no longer sufficient for protecting application data transmission due to exchanging shared keys generated via complex mathematical problems [13] and exposing user interactions on smart gadgets to outsiders [14].

Historically, academia and industry think of hardware devices as immutable structures that provide secure underpinning infrastructures behind cyberspace, which is not necessarily true. For instance, in August 2023, the National Institute of Standards and Technology (NIST) reported three hardware vulnerabilities (e.g., identified as CVE-2023-20583 [15], CVE-2022-40982, CVE-2023-20569 [16], and [17]), which are microcode bugs in billions of modern processors deployed in the cloud and personal computers (e.g., Intel and AMD). The existing network and computational resources are generally based on classical mechanics. In contrast, by applying the laws of quantum mechanics, the new generation of circuits (e.g., the Condor IBM machine with 1121 qubits [18]) could perform computations currently intractable even for classical supercomputers. Eventually, such breakthroughs in quantum hardware will allow industries to build sufficiently Large and Fault-Tolerant Quantum Computers (LFT-QC) in the near future. This accomplishment can significantly impact cyberspace security as the LFT-QC can break conventional asymmetric cryptosystems (e.g., Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC)) using the Shor's and Grover's algorithms [19].

In response to this threat, standards organizations such as NIST [20], the International Organization for Standardization (ISO) [21], and the Internet Engineering Task Force (IETF) [22] reported that existing security protocols are susceptible to quantum-based attacks. At the same time, they also investigated potential practical candidates and standardized PQC protocols in recent years. Theoretically, the PQC protocols rely on the intractability of complex mathematical problems such as lattice-based encryption or error-correction codes [23], designed to be implemented independently from physical principles and to ensure security resistance even in the quantum era. The real possibility of quantum-based cyberattacks corresponds to the fundamental security flaws of classical standard algorithms due to their dependency on mathematical problems that are known to be vulnerable to quantum-based attacks (e.g., large integer factorization, elliptic curve logarithm and its discrete counterpart [24]). In an ongoing threat in the post-quantum era named Harvest Now, Decrypt Later (HNDL) [25], also known as the Store-Now-Decrypt-Later (SNDL) or retrospective decryption, attackers can collect sensitive encrypted data from IoE-based systems and decode such collected data once the LFT-QC is accessible [11].

Therefore, following the thinking of many cybersecurity experts [11], we also believe that current e-governance policies should be reformed during the standardization fallacy so that they not only enforce the implementation of PQC protocols in IoE environments as soon as possible but also train netizens to learn up-to-date ways of safe interactions on smart gadgets through cyber-wellness (or digital media literacy) education programs [26]. As a paradigmatic example, when a user runs an application on a smartphone, (s)he may follow specific behavioral patterns to acquire e-services. Security protocols then involve multiple authentication processes to protect the confidentiality, privacy, and integrity of user data [14].

The current cyberspace lacks efficient e-governance policies to ensure that implementations of security schemes in the IoE environments

Table 1
Comparative analysis of existing surveys that have focused on reviewing security protocols in the post-quantum era.

Reference	i	ii	iii	Highlights (+) and limitations (–)
	Yes (✓) or No (×)			
Our study	✓	✓	✓	+ Implementation challenges of various standard security protocols in the post-quantum era were described. + Cyberattacks on different security protocols through the IoE environments were depicted. + Challenges of updating in-use security schemes to PQC protocols in IoE machines were discussed. + Strategic recommendations for practical and proactive actions by policy-makers were suggested.
Karakaya and Ulu (2024) [28]	◒	◒	×	+ Technical and theoretical challenges of PQC methods for edge computing security were described. + Potential theoretical research directions for future works were suggested. – Limited cyberattacks in IoE machines and cyberattacks on security protocols were discussed. – Lack of practical solutions for enhancing PQC protocols for edge computing in IoE environments.
Yang et al. (2023) [29]	◒	◒	×	+ A comprehensive overview and comparison of PQC approaches and quantum blockchains were provided. + Technical and theoretical of post-quantum blockchains, hybrid quantum blockchains, and fully quantum blockchains were discussed. – Limited vulnerabilities in IoE machines and cyberattacks on security protocols were considered. – Lack of practical solutions for implementing PQC protocols in IoE environments.
Gharavi et al. (2024) [30]	◒	◒	×	+ Technical and theoretical challenges of PQC methods for blockchain-based IoT applications were depicted. + Potential post-quantum blockchain-based solutions for IoT applications were discussed. – Limited vulnerabilities in IoE machines and cyberattacks on security protocols were considered. – Lack of practical solutions for implementing the PQC schemes in IoE environments.
Shekhawat and Gupta (2023) [31]	◒	◒	×	+ Technical and theoretical challenges of PQC protocols for smart grid networks were described. + Potential theoretical solutions for enhancing the PQC protocols for smart grid networks were suggested. – Limited vulnerabilities in IoE machines and cyberattacks on security protocols were considered. – Lack of practical solutions for implementing the PQC algorithms in IoE environments.
Chamola et al. (2021) [32]	×	◒	×	+ Technical and theoretical challenges of PQC protocols for 5G and beyond networks were described. + A summary of theoretical solutions for quantum key distribution protocols was suggested. – Lack of consideration of vulnerabilities in IoE machines and cyberattacks on security protocols. – Lack of practical solutions for implementing the PQC algorithms in IoE environments.

Note that ◒ represents the study that partially answers the above question.

align with standard instructions. That is why thousands of successful attacks compromised user information confidentiality, authenticity, and integrity. Such an issue is still an open problem even if recent standard PQC algorithms (e.g., CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+) [27] effectively secure data exchange over the IoE network due to the lack of enforcement policies to upgrade outdated protocols (e.g., TLS 1.2) and the exposure of user-to-machine interactions to outsiders. Therefore, cyberspace security practices require proactive transformations regarding e-governance standards and technical implementation guidelines for counteracting future side-channel and network attacks.

In this review article, we focus on answering the following three questions regarding the performance of standard security protocols in the post-quantum era: ***(i)*** What drives vulnerabilities through real IoE environments that put them at risk of being compromised by cyberattacks? ***(ii)*** What are the integration challenges of implementing PQC protocols in IoE environments? ***(iii)*** What are the potential strategic actions to reduce the transition procedure from classical security protocols to PQC approaches in the future of cyberspace? Table 1 compares existing survey studies with our article in the light of providing answers to the above three questions, as well as their contributions and limitations.

The rest of the paper is organized as follows. Section 2 describes different authentication schemes that are essential parts of security protocols. Section 3 explores the implementation challenges of standard security protocols, such as (D)TLS 1.3, when deployed in IoE environments. In Section 4, we discuss current technical obstacles that cause industries to keep the security protocols of the in-use IoE machines unupgraded. Section 5 explores the integration challenges of PQC protocols that practitioners face while deploying them in IoE environments. Section 6 depicts unprecedented risks of future cyberspace in the post-quantum era. Section 7 suggests potential strategies for decision-makers to address these issues through proactive e-governance policies. Finally, Section 8 summarizes the concluding remarks. The necessary acronyms/abbreviations and their definitions used in this article are depicted in Table 2.

2. Background on standard security protocols

In this section, we briefly describe various authentication schemes as the underpinning methods through the standard security protocols and cyberattacks on IoE systems.

2.1. Types of authentication schemes

As depicted in Fig. 1, standard security protocols comprise two types of authentication mechanisms: user-to-device (U2D) and device-to-device (D2D) (including device-to-gateway (D2G), device-to-server (D2S) and server-to-server (S2S)). In the following, we describe these approaches in detail.

2.1.1. U2D authentication

This is the first and most widely used technology for verifying user identity using credentials (e.g., PIN, password, hardware token, and biometrics) and thus granting access to smart gadgets or software systems in the IoE environment [33,34]. Unfortunately, most existing standard protocols focus only on ensuring D2D authentication and do not provide adequate U2D security due to the reusable nature of possession-, knowledge-, or biometrics-based credentials [7,14]. In public places (e.g., schools and airports), when a user enters the credentials on a smartphone, they can be subjected to side-channel attacks such as shoulder surfing, video recording, forged biometrics try, keystroke logging, downfall/inception [8], or remote timing and lattice [35]. On the adversarial side, malicious actors can perform an Advanced Persistent Threat (APT) to record the human interaction (e.g., screenshots or keylogs) through the device of the victim and then apply captured elements to defeat the security protocol [14].

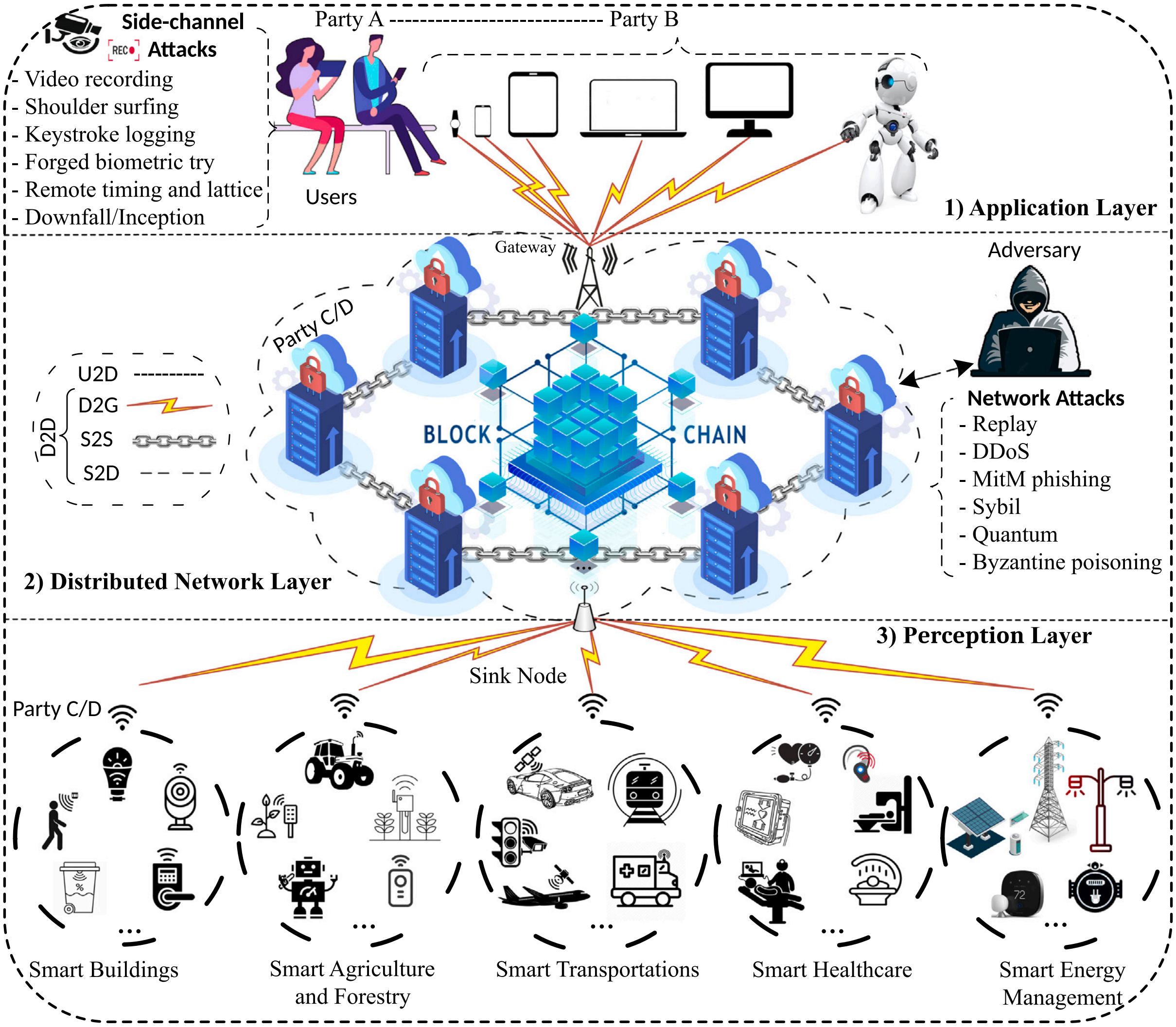


Fig. 1. An illustration of involved security protocols in the three-layered IoE architecture.

However, standard multi-factor authentication protocols (MFA) such as Universal 2nd Factor (U2F) [36] and Two-Factor Authentication (2FA) are more secure than conventional approaches. In practice, they combine a password with a hardware-based secret key (e.g., credit card) [37], which can be susceptible to keystroke logging, replay, and Man-in-the-Middle (MitM) phishing attacks [14]. Therefore, policy-makers must transform their frameworks to standardize dynamic and agile security protocols that function based on multiple one-time valid device-independent factors rather than using one or more static factors (e.g., hardware token or biometric) in next-generation MFA schemes.

2.1.2. D2D authentication

To secure the D2D authentication processes, developers typically apply various security protocols by implementing standard libraries (e.g., OpenSSL [38,39], and Tink [40]) as well as FIPS-certified APIs like the Bouncy Castle [41]. These are well-known open-source toolkits for implementing (D)TLS and QUIC UDP protocols. In particular, they can efficiently perform cryptographic approaches such as Advanced Encryption Standard (AES), Edwards-curve “Ed” or Elliptic-curve “EC” Digital Signature Algorithm (E(d/C)DSA, Elliptic-curve “EC” Diffie–Hellman Ephemeral ((EC)DHE), and Secure Hash Algorithm 3 (SHA-3) that were standardized by organizations such as NIST [20] and IETF [22] to achieve a desirable efficiency in terms of simplicity, flexibility, and key exchange resistance to side-channel attacks [42].

However, when a security protocol exchanges secret keys [44] as the partial aggregation of measurements to establish a secure connection between communicating machines, they are exposed to network attacks [45] (see Figs. 1 and 2). The ISO/IEC 2700X [21] family of standards provides implementation guidelines and practices for companies and organizations to keep their systems secure. Unfortunately, these guidelines partially provide practical solutions [46], which are not sufficient to fully address unprecedented cyberspace risks [43] due to existing flaws through standard security protocols (e.g., (D)LTS 1.2/3). Technically, (D)TLS protocols apply digital signatures (e.g., ECDSA in TLS 1.2) to authenticate the server and, in some cases, the client [47]. The digital signature is created by encrypting a message hash using the private key attached to the hashed message to prevent the MitM and Replay attacks. Some recent studies have proven that TLS 1.2 is vulnerable to private key leakage [48]. For instance, the work in [35] introduced a remote timing and lattice cryptanalysis attack in which the leak of the nonce in the ECDSA exchange process can lead to being hacked (e.g., the discovery of the private key) by the Lenstra–Lenstra–Lovász lattice basis reduction approach due to the weak randomness generation during the encryption process [49]. Later in October 2020 [50], the IETF recommended some improved pseudo-random number generators to address the weak randomness issue while implementing security protocols. However, implementing an actual random number generation is surprisingly challenging since no standardized or approved algorithm exists for classical computers to construct actual random numbers. It

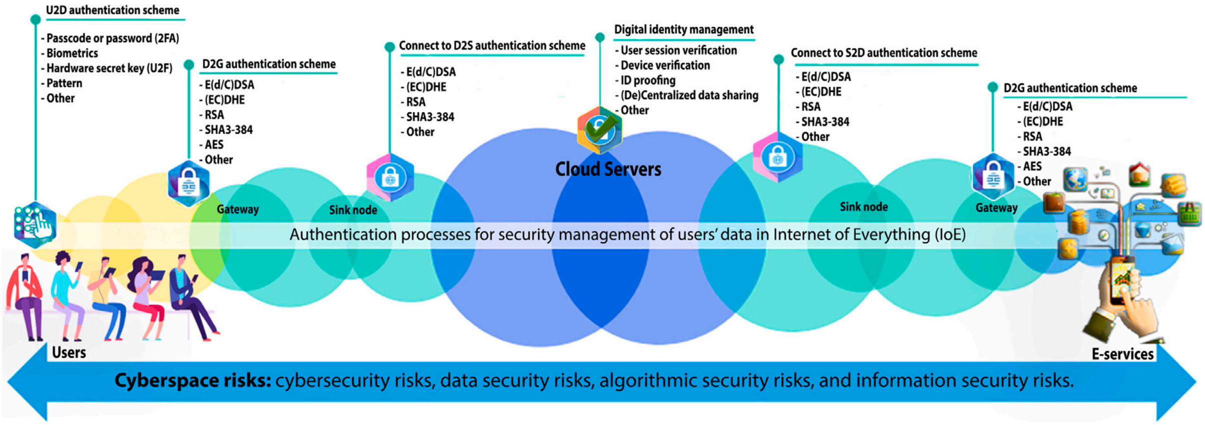

U2D authentication scheme
- Passcode or password (2FA)
- Biometrics
- Hardware secret key (U2F)
- Pattern
- Other
D2G authentication scheme
- E(d/C)DSA
- (EC)DHE
- RSA
- SHA3-384
- AES
- Other
Connect to D2S authentication scheme
- E(d/C)DSA
- (EC)DHE
- RSA
- SHA3-384
- Other
Digital identity management
- User session verification
- Device verification
- ID proofing
- (De)Centralized data sharing
- Other
Connect to S2D authentication scheme
- E(d/C)DSA
- (EC)DHE
- RSA
- SHA3-384
- Other
D2G authentication scheme
- E(d/C)DSA
- (EC)DHE
- RSA
- SHA3-384
- AES
- Other
Cloud Servers
Gateway
Sink node
Sink node
Gateway
Authentication processes for security management of users' data in Internet of Everything (IoE)
Users
E-services
Cyberspace risks: cybersecurity risks, data security risks, algorithmic security risks, and information security risks.

Fig. 2. Software-defined standard security protocols using authentication schemes and possible cyberspace risks [43].

Table 2
List of the most used acronyms/abbreviations.

Abbreviations	Description
GenAI	Generative Artificial Intelligence
IoE	Internet of Everything
PQC	Post-Quantum Cryptography
NIST	National Institute of Standards and Technology
ISO	International Organization for Standardization
IETF	Internet Engineering Task Force
LFT-QC	Large and Fault-Tolerant Quantum Computers
RSA	Rivest–Shamir–Adleman
ECC	Elliptic Curve Cryptography
HNDL	Harvest Now, Decrypt Later
SNDL	Store-Now-Decrypt-Later
U2D	User-to-Device
D2D	Device-to-Device
D2S	Device-to-Server
S2S	Server-to-Server
APT	Advanced persistent threat
MFA	multi-factor authentication
U2F	Universal 2nd Factor
2FA	Two Factor Authentication
MitM	Man-in-the-Middle
DDoS	Distributed Denial-of-Service
ECDSA	Elliptic Curve Digital Signature
EdDSA	Edwards-curve Digital Signature
ECDHE	Elliptic-curve Diffie–Hellman Ephemeral
SHA-3	Secure Hash Algorithm 3
PoW	Proof-of-work
PoUW	Proof-of-useful-work
TLS	Transport Layer Security
DTLS	Datagram Transport Layer Security
1-RTT	One Round Trip Time
MAC	Message Authentication Code
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
API	Application Programming Interface
AEAD	Authenticated Encryption with Associate Data
QPoUW	Quantum Proof-of-Useful-Work
QDPoS	Quantum Delegated Proof-of-Stake

is also worth remarking that using quantum mechanics, researchers at NIST have designed a certified random number generation approach that offers unpredictable randomness [51]. This method guarantees the unpredictability of its randomly constructed numbers and may improve the trust and security in cryptography systems.

According to the recent NIST side-channel vulnerability reports on August 15, 2023, they listed three significant hardware security flaws caused by information exposure bugs known as Inception and Collide+Power in multiple AMD processors (CVE-2023-20583 [15] and CVE-2023-20569 [16]) and Downfall in various types of Intel(R) CPUs (CVE-2022-40982 [17]). These vulnerabilities allow an adversary to steal sensitive credentials (e.g., passwords or encryption keys [8]).

To address the single-point-of-failure problem in centralized architectures, cybersecurity experts have introduced decentralized network-based technologies such as blockchain [52], distributed and federated learning [53,54], which function on each machine independently. Exploiting "local" federated learning nodes in a distributed manner, where they act as cooperative peers to authenticate communicating parties by encrypting all exchanged information using the hybrid PQC signature [55], may prevent the HNDL or SNDL quantum-based attack. In other words, data locality should be considered as an essential factor for future people-driven architectures to avoid leakages and maintain information sovereignty. Therefore, IoE-based systems process data using a decentralized model; hence, it does not fail once the central point is out of service. Because classical blockchains deploy the ECDSA and Merkle tree to verify blocks of transaction data, they are also vulnerable to side-channel and network attacks. To mitigate such threats, researchers introduced consensus approaches (e.g., proof-of-work (PoW) and Proof-of-stake (PoS)) to ensure the immutability of transactions.

Surprisingly, none of the consensus protocols guarantees the transactions' immutability in anonymous cryptocurrencies due to the possibility of a hard/soft fork. We believe that the above open vulnerabilities remain problematic in the post-quantum era. Hence, rather than relying on digital signatures and PQC algorithms, e-governance policymakers should introduce and standardize next-generation authentication schemes based on dynamic user credentials on a smart device to be continuously validated and exchanged between connected IoE machines.

2.2. Cyberattacks on IoE-based systems

Below, we classify realistic cyberattacks through IoE environments that can bypass security protocols via side-channels and network attacks.

(I) Side-channel attacks: This class of threats refers to an attempt to gain useful information for bypassing security protocols [14]. A side-channel can capture information useful to attack the security posture of a device or software through how an individual interacts with the consumer devices (e.g., screens, printers, or keyboards) or by exploiting unforeseen information leakages through them. Below, we briefly explain five of the most serious side-channel threats.

– Inception/Downfall: It is a recent zero-day cyberattack that makes AMD and Intel CPUs vulnerable to data theft through hardware security flaws. The "Inception" was disclosed by a group of researchers with the ETHZ [56] through AMD processors and later was announced by the NIST as the vulnerability CVE-2023-20569 on 8 August 2023. Similarly, the "Downfall" was discovered by Google researchers through Intel processors and publicly reported by the NIST as the vulnerability CVE-2022-40982 on 11 August 2023 [8]. Attackers can then steal sensitive information (e.g., passwords or encryption keys) using this backdoor, plaguing CPUs used in personal/cloud nodes [57].

– Camera recording or peeping: It is a cyber trick in which an attacker can use a camera to record the user entering his/her credentials on a device (see Fig. 1: “Party A”—“Party B”) and replicate them to bypass the U2D security protocol [14].

– Shoulder surfing: It is the act of watching a smart gadget (e.g., a phone) from a short distance to catch credentials while the user enters them. Similarly to the previous case, an attacker can replicate credentials to gain access [14].

– Keystroke logging or Keylogging: It is an umbrella for various forms of hidden mal(spy)ware (e.g., Remote Access Trojan (RAT)) that records what a user types on his/her gadget (e.g., PIN or password) and smuggles it to a remote attacker. The keylogger could be dropped via phishing emails, instant messages, or social media posts [14]. An attacker can also “simply” extract the user’s credentials from the logs and replicate them to bypass the U2D security protocol once (s)he gets hold of the user’s device. For example, Glupteba [58] is a blockchain-based malware botnet that was first discovered in 2018 and is still active today. This botnet is an ongoing serious threat due to its decentralized source, which allows it to act as a rootkit, stealer, and cryptojacker through browsers.

– Forged biometric try: It is a cyber trap in which an attacker collects various biometrics information belonging to the victim and exploits them to generate fake objects with authentic biometric traits (e.g., a plastic finger generated using a 3D printer) [14].

– Remote timing and lattice: It aims at extracting a private key of the ECDSA signature from commodity computers, by searching for lattices from the encrypted data due to the weak randomness issue. An attacker can apply a discovered PRK to decrypt the encrypted data (e.g., (D)TLS 1.2 Handshake). This is the main reason that the ECDSA is invalid in the (D)TLS 1.3 due to the re-usability flaw of the static shared key [8].

(II) Network attacks: In the IoE network, the (D)TLS or CoAP protocols establish a secure channel between two nodes to exchange information safely. As said, encrypting authentication information does not guarantee the security, confidentiality, and integrity of transmitted messages since attackers can steal the shared key between communicating parties [59]. Below, we summarize five network-based severe attacks.

– Man-in-the-Middle (MitM): It involves a malicious party injecting the device of an attacker virtually inside the connection between two IoE machines by performing some traps such as IP spoofing or DNS cache poisoning. The ultimate goal of this class of threats is to monitor network traffic to steal sensitive information, such as (D)TLS Handshake requests from IoE network packets [32].

– Replay: It occurs when a malicious intruder takes advantage of a security flaw to capture the authentication information and its subsequent retransmission for gaining unauthorized access to a secure channel (e.g., session resumption of (D)TLS 1.2/1.3). Here, an attacker is not even required to decrypt such data if (s)he successfully catches the authentication information [60].

– Distributed Denial-of-Service (DDoS): It exploits a flood of network traffic to overwhelm IoE machines or their surrounding infrastructures that were infected by a set of remotely controllable botnets. A notable example of such attacks is Mirai [14]. In general, network resources (e.g., at gateways or web servers) allow a bounded number of access requests by other machines, which they expect to receive real-time services simultaneously. In addition to restricting the capacity of the IoE nodes, communication between a device and a server has limited bandwidth. Thus, if the capacity of any component of the network infrastructure reaches the maximum number of requests, the quality of service will be reduced as follows: (i) some or all requests, even from legitimate sources, may be ignored; (ii) the reply to requests will be much slower than when the device is in normal condition. In such a case, an attacker floods a server with massive Internet traffic to prevent users from establishing a secure channel and accessing e-services correctly [31].

– Sybil: It represents a malicious intruder trying to take control of the IoE network via multiple fabricated nodes (both forged or Sybil) to outvote authentic ones. Thus, they can refuse fake accounts to transmit or receive blocks effectively by obstructing other users through the same network [61]. In the case of large-scale Sybil cyberattacks, they can occupy most of the computing power (e.g., the hash rate in the blockchain networks) and modify the ordering of transactions to prevent them from being confirmed. For example, such attempts can even reverse the data blocks while in control, performing double-spending transactions [28].

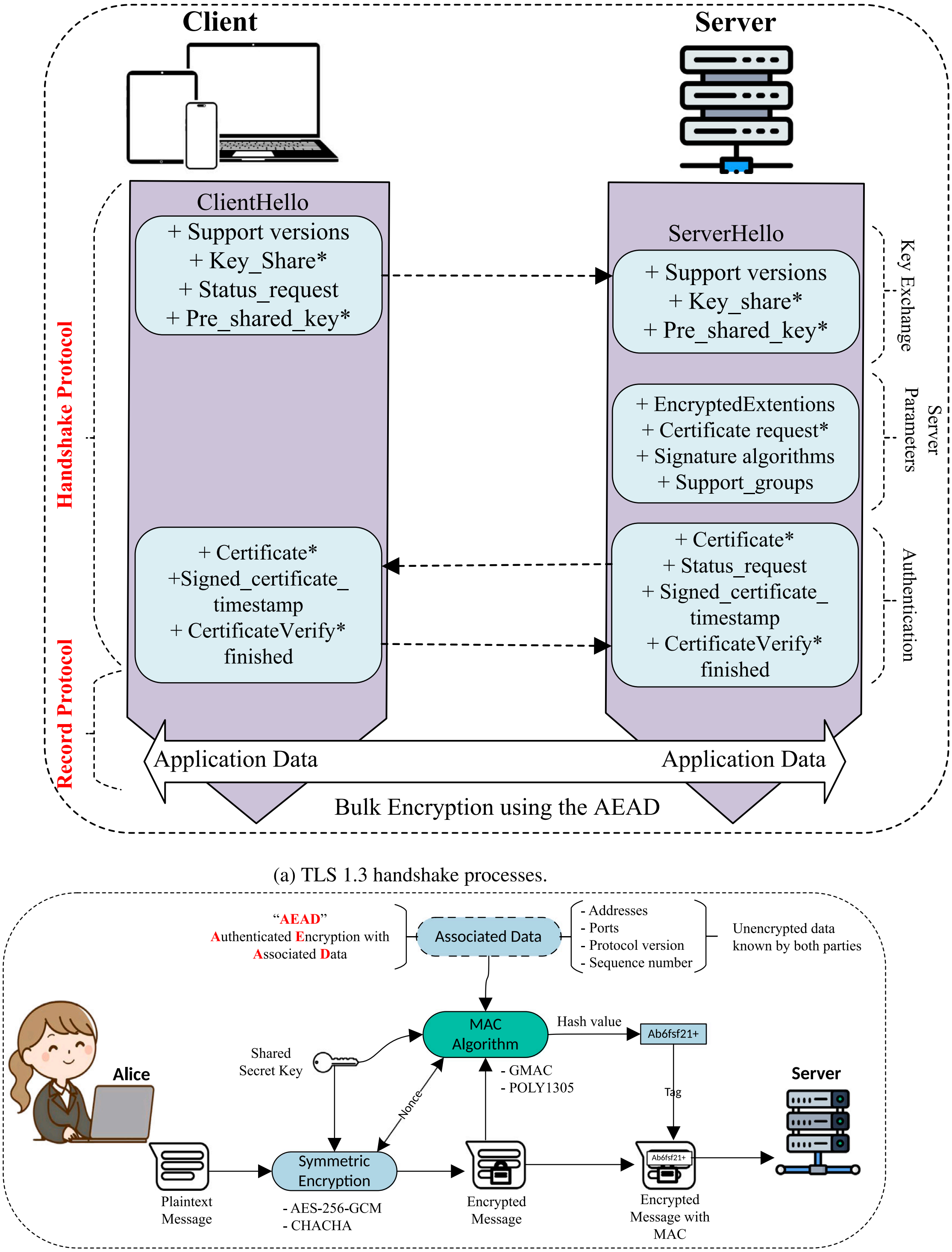
– Quantum-based: It is the quintessential exploitation of the “capturing or stealing data now and decrypting it later” paradigm, where attackers employ intelligent data mining technologies to collect encrypted information. To implement such an offensive model, Shor’s and Grover’s algorithms [30] play a major role. Specifically, Shor’s algorithm can efficiently find the prime factors in an encryption key, which compromises the underpinning foundations of most classical cryptographic approaches (e.g., RSA and ECDSA [62]). In addition, Grover’s algorithm can perform a quadratic speedup in unstructured search, which poses a serious threat to the hash functions (e.g., SHA-2/3) deployed in connecting blocks within blockchain networks. In response to these issues, researchers have been actively investigating proactive solutions to prevent quantum-based attacks by integrating PQC protocols in blockchains [29].

– Byzantine poisoning: it is performed by a set of fully trusted nodes in a distributed network that already have passed all the authentication processes, which can be turned into malicious machines [63]. Technically, each node can execute data poisoning through the blockchain-based systems and federated learning models in IoE-based systems [64].

3. Implementation challenges of standard security protocols

The Secure Sockets Layer (SSL) v2 was publicly released by Netscape in 1995 as a standard protocol for securing Internet connections between two machines (e.g., computers and servers) and safeguarding any sensitive data transmitted between them. The main goal was to prevent attackers from tampering, eavesdropping, or monitoring exchanged information, such as banking credentials. Later, in the 1995–1999 period, Netscape introduced several versions, and IETF (1999–2018) named (D)TLS 1.X to address security flaws in former ones [65]. The latter variants must comply with the previous versions for a certain period. Currently, TLS 1.2 and 1.3 are valid versions that can be implemented via standard Application Programming Interfaces (APIs). Therefore, it is recommended that industries upgrade their infrastructure to integrate (D)TLS 1.3 [66]. Note that the versions before TLS 1.2 have been deprecated due to security flaws discovered in the deployed cryptosystems. In practice, TLS 1.2/3 establishes a secure channel considering the type of e-service between two parties: a client (e.g., a browser on a smartphone) and a web server [67]. For backward compatibility with previous versions, TLS 1.2 supports several cipher suites, which can be executed by earlier versions and offers a configurable selection of weak cryptographic protocols prone to severe attacks, such as MitM and Replay [12]. Although TLS 1.3 is theoretically proven to be secure, most existing implementations (e.g., OpenSSL [38] or JSSE [68]) partially support the security characteristics of TLS 1.3 [69], which causes backward compatibility issues and opens opportunities for downgrade actions [70], i.e., needing to drop to the TLS 1.2, which is technically a less secure version and more vulnerable to cyberattcks. Fig. 3 depicts the process of establishing a secure channel and exchanging application data between two parties using the TLS 1.3 [22,68].

As depicted in Fig. 3(a), TLS 1.3 utilizes a handshake protocol to establish a secure channel and record protocol to safely transfer the application data between two communicating parties over the IoE



(a) TLS 1.3 handshake processes.

(b) Bulk encryption using the AEAD algorithms.

Fig. 3. An illustration of establishing a secure channel between client and server using the TLS 1.3 handshake and record protocols. Note that '+' represents extensions or parameters exchanged between two parties, and '*' denotes situation-dependent or optional items.

networks. In the following, we briefly explain these two protocols in detail.

(I) Handshake Protocol: This phase is responsible for authenticating two parties and generating a shared key using two groups of asymmetric cryptography algorithms (e.g., X25519 or NIST Curve P-256) [38]. The record protocol utilizes the constructed shared key during handshakes to encode the application data or perform bulk encryption. Technically, the number of handshake steps depends on the history of the connection modes between two parties that the client and the server experienced [71]. Below, we summarize these two modes and their impacts on handshake steps.

(1) One Round Trip Time (1–RTT) Mode: If a client visits a server for the first time [22], then TLS 1.3 performs the 1-RTT mode, which exchanges two messages: ClientHello and ServerHello as the handshake steps (see Fig. 3(a)), before starting the application data transmission [72].

– *ClientHello:* This is the first message a client device sends to the server to negotiate the TLS version (specific types of cipher suits or cryptography protocols), and the transmission modes [70] that determine when the client transfers the encrypted application data to the server after the **shared key** is generated [12]. This shared key is stored in the client and server as the **pre_shared_key**, which will be deployed for future communications in resumption mode, which speeds up the establishment of the secure channel in the next tries. Table 3 lists the key exchange protocols and digital signatures that can be performed during this phase.

– *ServerHello:* Once the server receives the client hello, it sends a ServerHello message as a response to received extensions or parameters within the ClientHello accordingly [68]. Note that the server must execute similar cipher suits (see Table 3) to decrypt and re-encrypt the exchanged extensions and certificates (e.g., X.509) [73,74].

(2) Zero Round Trip Time Resumption (0–RTT) Mode: If a client has recently visited a server and holds a pre_shared_key, then TLS 1.3 enables the client and server to transfer data in the first messages to each other without requiring the handshake process [75]. Although this mode generally decreases communication latency, it opens opportunities for replay attacks [68]. According to the RFC8446 [22], 0-RTT mode normally imitates the security characteristics of 1-RTT in TLS 1.3 by having two exceptions: (i) the 0-RTT encryption keys do not follow full forward secrecy mechanism [76], and (ii) the server cannot ensure the "non-replayability" or "uniqueness" of the handshake process without storing undue amounts of state. For instance, the Google team enabled TLS 1.3 by default for all TLS communications in Android 10+ (e.g., API level 29+), which does not support the 0-RTT mode [77] to prevent the Replay and MitM attacks. Note that the (D)TLS 1.3 applies the most efficient standard digital signature (e.g., Ed25519) to sign entire handshakes [78], which prevents client/server certificates from being compromised by MitM attacks considering the 1-RTT mode. Nevertheless, once the 0-RTT mode is performed, it leaves the pre_shared_key susceptible to replay attack.

(II) Record Protocol: This phase is responsible for bulk encryption using standard symmetric-key approaches (e.g., 0 × 1303), ensuring the integrity and confidentiality [79] of application data while transmitted via an insecure network channel. This protocol uses the Authenticated Encryption with Associate Data (AEAD) algorithms [80] (see Fig. 3(b)) for verifying the messages against tampering and unauthorized access by malicious parties. These mechanisms require a one-time valid nonce (e.g., a time-stamp), associated data, and a hash value to be applied with the message authentication code (MAC) and the key derivation function [22].

In general, DTLS 1.2/3 [81,82] is an adaptation of the TLS 1.2/1.3 for the User Datagram Protocol (UDP), while TLS 1.2/3 is developed to operate on top of the Transmission Control Protocol (TCP) [83]. In some cases, it is necessary to keep the security algorithms to a minimum to protect the infrastructure and source code. Hence, DTLS was designed to provide the same security measures as TLS to lower the requirement for deploying "IPsec" or developing a custom mechanism. In addition, the primary difference between these protocols is that DTLS is built on top of the UDP, while the TLS functions based on the TCP. For instance, DTLS is typically utilized for securing the IoT machines, gaming, VPNs, voice call traffic via broadband Internet, and streaming using lightweight cryptographic methods (e.g., ASCON family) [84]. Note that the (D)TLS 1.2 and 1.3 are the currently valid standard protocols that secure data exchanged for multiple applications, including Hypertext Transfer Protocol (HTTP), File Transfer Protocol, Internet Message Access Protocol, Simple Mail Transfer Protocol (SMTP), the Extensible Messaging and Presence Protocol, etc. [83]. However, the TLS and DTLS features have transformed over the years, and later variants optimized the security protocol and simultaneously improved characteristics (often by applying the extensions), while some functionality was eliminated without substitute [85]. The option for updating the initialization vectors and encryption keys has been added in TLS 1.3 in a later stage, i.e., in RFC 8446bis [22] by deploying the KeyUpdate message, which is intended to (partially) substitute the renegotiation from earlier TLS versions. While complex, the renegotiation option provided the necessary functionality no longer supported by TLS 1.3, consisting of updating master keys using the DHE method during a session's lifetime.

In IoE-based networks, there are particular use cases of the (D)TLS where long-lived sessions are necessary. In such cases, availability is essential, and a connection interruption due to periodic session resumptions is not an option. Re-establishing a handshake using the (EC)DHE and swamping from the old to the new session might be an alternative for particular applications. Still, it causes complexity and influences the overall performance, which may lead to service interruption [85].

Furthermore, to secure constrained IoE devices, the cybersecurity experts standardized the Object Security for Constrained RESTful Environments (OSCORE) protocol [90] to guarantee end-to-end security for Constrained Application Protocol (CoAP) messages at the application layer. However, due to the necessity to exchange static shared keys generated by symmetric key algorithms through the network channel when CoAP is deployed in IoE edge devices (e.g., D2G), they are technically susceptible to replay, and MitM attacks [91]. In addition, in some past IoE deployments, the implementations have utilized the IPsec to secure the communication channels and recently switched to (D)TLS. To reduce the risks of key compromise, the necessity for cryptographic key updates in an existing session has become a requirement, which was considered in the recent changes of TLS 1.3 in October 2024 [85].

4. Update problems of in-use IoE machines

Although the LFT-QC are in their infancy, they pose an inevitable threat to state-of-the-art cryptography protocols [11] that may put classical ECC-based methods and hash functions at risk of being compromised [24]. Even future standard PQC algorithms [27] could address this issue only partially. Considering recent advances in quantum computing, it is highly probable that LFT-QC will be connected to the IoE environments soon (e.g., in five years). Hence, a complex problem arises as a considerable number of IoE machines deploy former standard protocols such as CoAP or TLS 1.2/1.3, which put them at risk of data breaches against side-channel and network attacks [35,45,94]. According to the recent updates of the (D)TLS 1.3 in October 2024 [85], the recently added specification of (D)TLS 1.3 defines a novel, extended key update message, which supports perfect forward secrecy. This feature functions by deploying a Diffie–Hellman exchange based on the cipher suits agreed upon during the initial exchange. The functionality of this extension is supported by the (D)TLS flags extension approach. This idea requires re-establishing extended key updates during the Handshake, which forces attackers to perform dynamic key exfiltration for unauthorized access attempts. In addition to the (D)TLS key updates, for the IPsec, the German BSI, the NIST, and the French ANSSI have requested to include the implementations of the Diffie–Hellman exchanges frequently for comprising the forward secrecy, which forces the attackers to execute a dynamic key extraction if they aim to breach the communication channel. While IPsec/IKEv2 provides the desired functionality, DevOps engineers often deploy the (D)TLS for simplifying the integration in cloud-based IoE environments.

In fact, updating current in-use IoE machines with the standard PQC protocols is a complex problem that requires a lot of resources, which is time-intensive and costly [95]. According to an empirical study by Enterprise Management Associates in 2022 (sponsored by F5 and Cisco) [96], researchers explored the actual implementation of TLS 1.3 [22] in the IoE environments four years after its release date by surveying the sentiments of 208 technology leaders in North America across industries (e.g., e-services, healthcare, and finance) [97]. They

Table 3
Practical implications of standard security protocols in IoE environments.

Versions	Handshake protocol	Record protocol	Highlights (+) and Limitations (−)
(D)TLS 1.2 Released: 2008 [86], [83]	• RSA (0 × 009c, 0 × 009d, 0 × 002f, or 0 × 0035) • ECDHE (0xc02f, 0xc030, 0xc013, or 0xc014) • ECDSA (0xcca9, 0xc02b, or 0xc02c)	• AES_128_GCM_SHA256 (0 × 1301) • AES_256_GCM_SHA384 (0 × 1302) • CHACHA20_POLY1305_SHA256 (0 × 1303)	+ Compatible with a wide range of cryptographic algorithms + Applying AEAD algorithms to provide confidentiality and integrity − Allowing communicating parties to use weak protocols − Renegotiation flaw as Client certificate is not encrypted − Static key exchange algorithms that are easy to be replayed − Vulnerability of ECDSA against side-channel attacks − 2-RTT handshakes are required to generate the shared key
(D)TLS 1.3 Released: 2018 [22], [83], [87] Updated: 2024 [55], [88], [89]	• (EC)DHE (0 × 25519 or NIST P-256) • EdDSA (Ed25519 or Ed488) • Perfect Forward Secrecy (1-RTT) • Hybrid PQC key exchange (X25519Kyber768)	• AES_128_GCM_SHA256 (0 × 1301) • AES_256_GCM_SHA384 (0 × 1302) • CHACHA20_POLY1305_SHA256 (0 × 1303) • Empty_RENEGOTIATION_INFO (0 × 00ff) • ECDH-NISTP256-Kyber-512r3-SHA256 • ECDH-NISTP384-Kyber-768R3-SHA384 • ECDH-NISTP521-Kyber-1024R3-SHA512 • X25519-Kyber-512R3-SHA256 • ML-KEM-512 (0 × 0200), ML-KEM-768 (0 × 0201) and ML-KEM-1024 (0 × 0202)	+ Faster handshake protocol (1-RTT) that reduces the latency + More secure AEAD algorithms based on dynamic secret keys + All the handshake messages are signed by the EdDSA or hybrid PQC + Initiating the renegotiation information to mitigate replay attacks − Incompatibility with the former cryptography algorithms − 0-RTT session resumption flaw that can be easily replayed
OSCORE Released: 2019 [90], [91], [92], [93]	• ECDH (SS+HKDF-256/512 or A256 kW) • ECDSA (SHA-256 and P-256) • EdDSA (Ed25519)	• AES-CCM-16-64-128 • AES-128-GCM • Chacha20/Poly1305-256	+ Light-weight cryptography methods for constrained IoE devices + Applying AEAD using HMAK-based HKDF − Static ECDH-based key-exchange approaches − Vulnerable to reply and MitM attacks − Allowing more than two parties access a shared key

Note that '+' indicates the advantages that a particular protocol offers, '−' represents its constraints, and '•' compatible/supportable cipher suites by each security protocol.

concluded that only 76.2% of the respondents implemented TLS 1.3 to secure the traffic of employees working remotely, while 40.6% needed significant infrastructure upgrades to accommodate integration. Among the 208 participants, 96% have paused their implementations due to loss of visibility in traffic, and 44% were forced to downgrade to TLS 1.2 considering the issues depicted in Fig. 4. This statement raises the question: How would the NIST and IETF organizations ensure that all private companies worldwide update their IoE-based systems with new (D)TLS 1.3 protocols? The answer is that only a global commission [98] could manage, enforce, and ensure this transition by introducing e-governance standards for the sustainability and resilience of cyberspace security.

5. Post-quantum cryptography uncertainties

The lack of sufficient PQC implementations to protect IoE environments against quantum-based attacks remains an ongoing concern among cybersecurity activists. During the past decade, standard organizations (e.g., IETF and NIST) have taken considerable promising steps toward the risk assessment, planning, and implementation of PQC approaches [27] to mitigate the possible upcoming quantum-based threats that led to the standardization of four PQC protocols such as CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium, FALCON, and SPHINCS$^+$ for digital signatures. These PQC protocols are the results of eight years of practical investigations managed by the NIST. This agency has organized three rounds of competitions from 2017–2022 and rallied the world's cryptography specialists to devise, submit, and assess encryption approaches that can resist quantum-based attacks [99].

Later, in March 2023, IETF published several technical guidelines to implement a hybrid PQC key exchange mechanism called X25519Kyber768 for TLS 1.3 [55,88]. However, it has not yet been implemented effectively and efficiently and appears exploratory, considering compatibility issues of TLS 1.3. For instance, the Google team has taken the first action by releasing Chrome version 116 in August 2023, which deploys hybrid PQC key agreements (e.g., X25519Kyber768) in their TLS 1.3 implementation [100]. The advances pursued by industry and academia in quantum computing technologies (e.g., superconducting qubits [101]) have dramatically increased. Several quantum machines were built by companies such as Google, IBM, and Intel [102] that recently passed the significant milestone, i.e., "quantum calculation on a scale where classical computers will struggle" [103] to perform. For example, according to Google's report on the quantum AI team in April 2023 [104], they experimented with a complex problem on the 67-qubit next-gen Sycamore processor [105], which requires the Frontier, the most powerful supercomputer in the world, to process it almost 47.2 years of computations to reach the same result. In addition, other quantum companies such as Rigetti [106], D-Wave [107], and IonQ [108] have regularly reported their progressive achievements in the form of quantum machines and software development kits. These breakthroughs enable various applications such as quantum machine learning and generative AI [109], quantum blockchains [29], quantum key distribution networks [110], and quantum as a service [111]. Among such an extensive range of applications, we have witnessed novel approaches for hyper-scale machine learning (e.g., quantum annealing [112]), modern quantum-safe exchange secret keys [110], and various quantum related-key differential cryptanalysis [113,114] approaches to accessing a quantum system (e.g., remote quantum labs [115] or simulators [116,117]). Furthermore, several cloud service providers (e.g., Amazon's Bracket [118] and Microsoft's Azure [119]) have begun to offer services based on quantum computing for research practices.

Indeed, such breakthroughs draw promising signs toward building the LFT-QC that can execute Shor's and Grover's algorithms [19] to break many in-use standard cryptography protocols in IoE environments [120]. Once the LFT-QC are connected to IoE networks, they can eventually compromise data integrity and confidentiality of communications within cyberspace [121]. In other words, LFT-QC can perform Shor's algorithm for solving significant mathematical problems that break static key ECC-based methods, particularly those that function according to the discrete logarithm problem in groups of points of elliptic curves or multiplicative sets of finite fields. These mathematical methods are still a significant part of standard security protocols that are used in most implemented D2D authentications (e.g., (D)TLS 1.2) over IoE environments [122]. In the literature, some studies such as [123–126], and [127] suggested novel scalable hardware architectures, which feature secure and efficient implementations

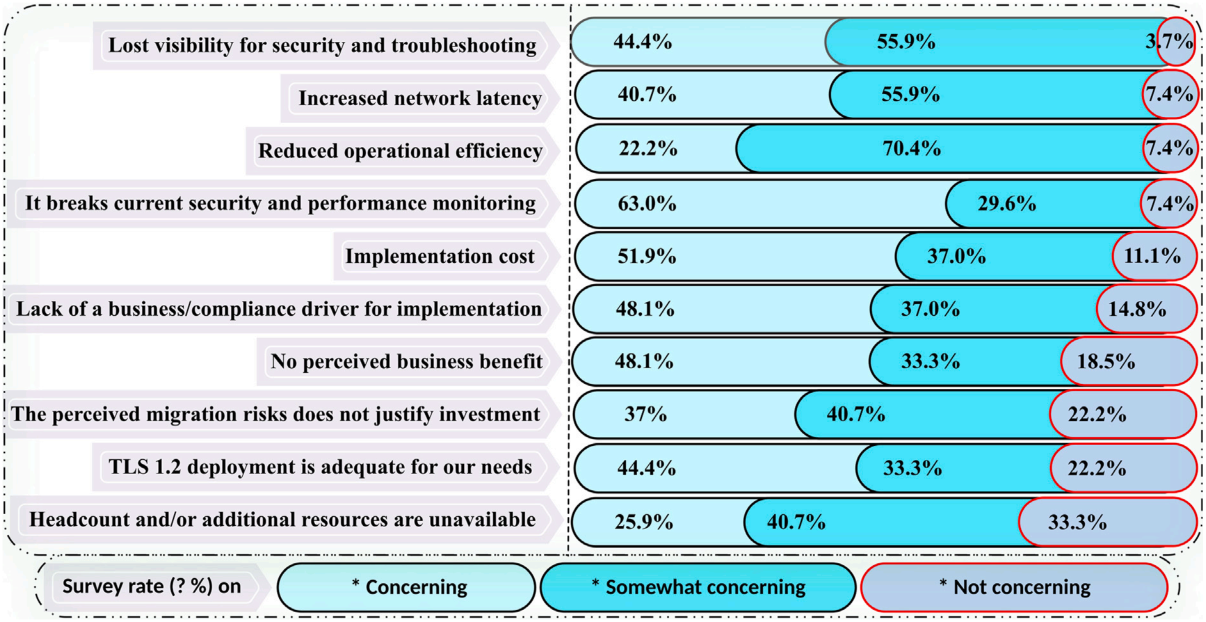


Fig. 4. List of issues rated by survey participants why they would not implement the TLS 1.3.

of cryptographic approaches that could be applied to enhance the performance of PQC protocols. In addition, some other research works, such as [128–132], and [133], have investigated the efficiency of fault (or error) detection schemes for number theoretic transform and lightweight PQC protocols in IoE machines, which enable efficient implementations by allowing for more flexible option of PQC parameters. Besides, some experimental studies such as [87,134], and [135] have investigated secure implementations of classical cryptographic signatures (e.g., Ed25519) that optimize communication latency and reduce resource utilization for deploying ECC-based security protocols in constrained IoE devices. Moreover, recent investigations, such as [74, 135], and [136] have considered multiple classical and PQC primitives and explored implementation mechanisms for performing hybrid D2D authentication. Practically, these optimized implementations can contribute to the transition from classical cryptographic protocols to PQC algorithms.

As the permissionless blockchains (e.g., Bitcoin and Ethereum) are publicly open to anyone, any device can join the network and remain anonymous. An unknown IoE machine may intercept and tamper with blocks to compromise the blockchain network. Thus, the blockchain network faces a challenging state called *a fork*. For instance, a fork within a specific chain consists of tampered data, while other chains include authentic records of transactions. Technically, the decentralized nature of blockchains needs a unique consensus protocol (e.g., PoW or PoS) to verify the authenticity of transaction data, whereby nodes agree on the contemporary state of the ledger. In other words, a consensus mechanism should prevent such forks so that anyone complies with a single variant of truth. In contrast, in private blockchains, although participating nodes are selected and known, consensus protocols are still needed as the backbone of decentralized computing systems, enabling several IoE devices to work with each other cohesively. Consensus protocols also allow agreement on distributed data through encrypted processes, improving fault tolerance and reliability of the blockchain networks. Also, there is a possibility that the nodes cannot be trustworthy — this state is called the Byzantine Generals Problem [29,63]. In practice, the practical implementations of consensus algorithms in blockchains are challenging, whereas the IoE devices are either faulty or incapable of communicating reliably. This paradox is also known as the Two Generals' problem, a classic insoluble issue in distributed systems that require consensus algorithms through an unreliable network [54]. To address such issues and enrich post-quantum attack-resistance of the blockchain-driven Web 3.0 ecosystem, researchers and experts adopted PQC algorithms to ensure the security and privacy of netizens [137], consisting of quantum-based block propagation, novel consensus mechanisms (e.g., quantum PoUW (QPoUW) [138] and quantum delegated PoS (QDPoS) [139]), quantum block verification, and identity authentication (see Fig. 5). However, such quantum-empowered security protocols are in exploratory stages, and their implementations in the current Web 3.0 ecosystem are complex because the existing IoE infrastructures need to be upgraded so that they support necessary quantum computing structures.

6. Unprecedented risks of cyberspace

In general, the connectivity of digital things in IoE environments provides valuable e-services that improves people's daily lives by exploring them through gadgets such as smartphones, computers, and tablets. On the other hand, the advents of LFT-QC and GenAI large multi-modal models empower unprecedented cyberthreats. Below, we summarize ongoing and future cyberspace risks, which represent the main lessons learned from our study.

6.1. Socio-economic and technological risks

According to two recent reports published by Statista in 2023 [140, 141], cyberattacks caused losses of billions of dollars (see Fig. 6(a)). Moreover, according to the Chainalysis crypto crime report in January 2024 [142], they discovered more than 20 billion annual cryptocurrency transactions that were received via illicit addresses from 2021–2023 associated with cybercrimes such as crypto scamming schemes, APTs, ransomware, and the dark web markets (see Fig. 6). In addition, according to the TRM Labs' report in July 2024 [143], the hackers managed to steal $1.38 billion in the first half of 2024 from several exchange platforms (e.g., DMM Bitcoin [144]). Technically, one of the main reasons behind the successful attacks mentioned above is the fact that the attackers can perform APTs on users' devices to steal cryptocurrency wallets' private keys and seed phrases or other sensitive information [145]. For executing the APTs, malicious actors deploy continuous and sophisticated hacking approaches (e.g., installing stegomalware [146] or sharing deepfake phishing advertisements [147])

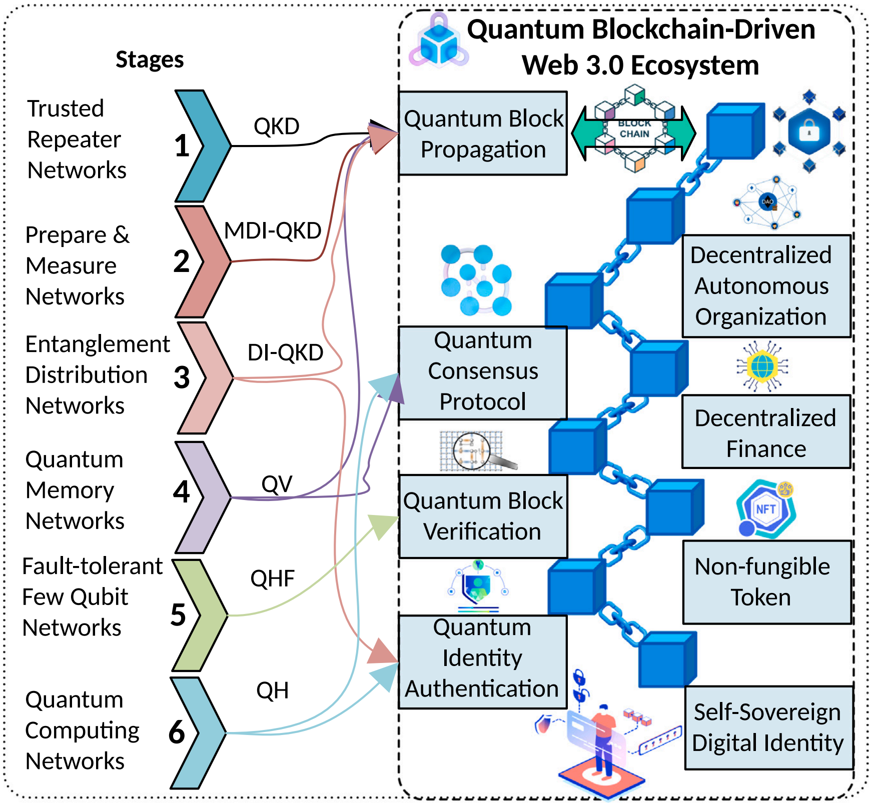

Stages
Quantum Blockchain-Driven Web 3.0 Ecosystem
Trusted Repeater Networks
1
QKD
Prepare & Measure Networks
2
MDI-QKD
Entanglement Distribution Networks
3
DI-QKD
Quantum Memory Networks
4
QV
Fault-tolerant Few Qubit Networks
5
QHF
Quantum Computing Networks
6
QH
Quantum Block Propagation
BLOCK CHAIN
Decentralized Autonomous Organization
Quantum Consensus Protocol
Decentralized Finance
Quantum Block Verification
NFT
Non-fungible Token
Quantum Identity Authentication
Self-Sovereign Digital Identity

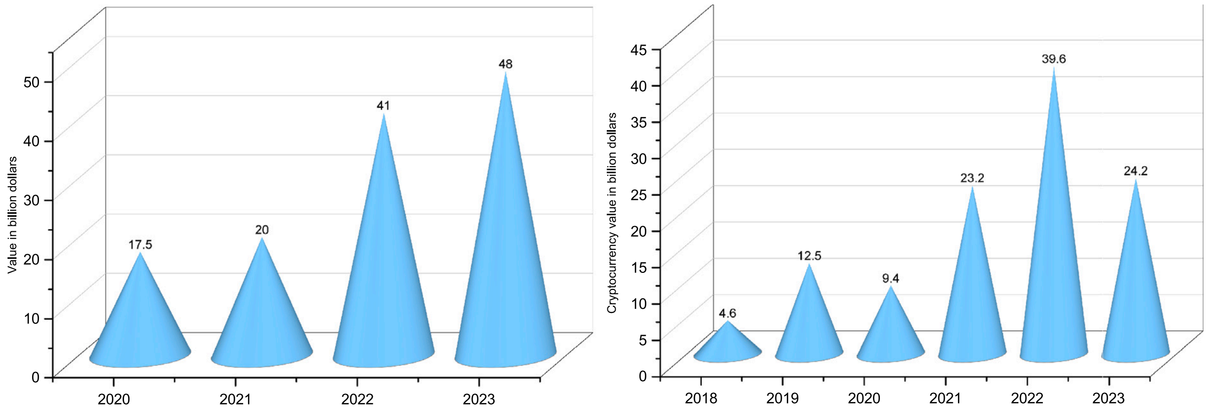
Fig. 5. Development stages of hybrid quantum blockchain-driven Web 3.0 ecosystem. Abbreviations are as follows: quantum key distribution (QKD), measurement device independent (MDI), device-independent (DI), quantum voting (QV), quantum hash function (QHF), and quantum hypergraph (QH) [137].

to access an IoE machine and remain hidden inside it for a long time. For instance, victims are induced to interact with seemingly legitimate deepfake phishing ads, cryptogames, or websites or download clipper malware (e.g., keyloggers) infected with malicious codes [148]. Then, attackers could steal the victims' security credentials and apply them to access their cryptocurrency wallets, drain their funds, or collect other sensitive information from their devices.

In addition to the aforementioned ongoing cyberthreats, the next future suggests the presence of robots able to monitor real-world events by collecting sensory data from various IoE devices. Hence, they can analyze real-time data using local or distributed IoE systems to identify the best action for the situation. These IoE layers can then send commands to networked robots to control objects in the physical world. This networked set of IoE machines has been named as the *Internet of Robotic Things (IoRT)* [149]. What may happen to our physical world if the authentication schemes in this IoRT are not sufficiently secure to prevent cyberattacks? The answer is that robots could execute unexpected actions by risking human lives or impacting the behavior of significant parts of a smart city.

In today's cyberspace, the above-discussed network cyberattacks allow an adversary to compromise blockchain networks [45]. For instance, a Sybil attacker creates several fabricated network nodes. By exploiting these nodes, (s)he can gain majority consensus and control blockchain transactions in the process. Similarly, DDoS attacks (e.g., ShellBot [150] spread crypto miners) flood blockchain networks with false and spam transactions, allowing adversaries to compromise the access of authentic users [151]. On each end-point (e.g., smartphone), the attacker may run spyware as a MitM phishing trap (e.g., Evilginx) [152] using URLs similar to the victim's destination, i.e., directing the trapped user to a reverse proxy server. Then, (s)he utilizes the proxy server to intercept the connection between the actual web server and the client's device. Additionally, it employs a TLS certificate [153] created by the attacker, allowing full HTTPS decryption that enables an opportunity to steal sensitive information [14].

Another cyberattack called replay occurs when systems leveraging the blockchain upgrade or alter their cryptographic protocols, i.e., a process known as a hard/soft fork. By performing this attack, intruders capture encrypted data during transmission and apply it to deceive the blockchain into committing the same transaction multiple times, known as double-spending [154]. In theory, one of the primary objectives of the blockchain is to transform transactional security by providing traceability and transparency features. Unfortunately, it also empowers hard-to-trace technologies that create and exchange anonymous cryptocurrencies (e.g., Bitcoin and Ethereum) often deployed in dark web marketplaces. Consequently, anonymity behind such systems risks increasing cybercrimes such as money laundering [155], human trafficking, and ransomware attacks [156,157]. For instance, according to a recent report published by Bitdefender in January 2023 [158], a surprisingly rudimentary attack vector named address poisoning allows malicious actors to divert real-time transactions to their wallet addresses as the destination by tampering with them, embedding bogus data, or altering routing tables. This attack deploys various approaches (e.g., performing spyware like Glupteba) to undermine the security and integrity of transactions to either steal cryptocurrencies or damage the regular operation of blockchain networks. For instance, the Google security team tried to take the Glupteba botnet down for the first time in December 2021 [159]. Later in June 2024, the CheckPoint research team reported that the Glupteba had been active since 2019 [160] due to its ability to resist shutdown attempts. In fact, it deploys a C&C address update mechanism by taking advantage of public Bitcoin lists, which cannot be easily blocked or filtered. This statement implies that blockchain-based malware can replicate a copy of their source on all the connected chains and is almost impossible to take down due to the nature of distributed ledgers.



(a) Predicated losses via online payment fraud worldwide. (b) Cryptoassets value received by illicit cryptocurrency addresses.

Fig. 6. Estimated statistical analysis of financial losses through cyberspace from 2018–2023 [141,142].

6.2. Environmental risks

In addition to the risks mentioned above, blockchain-based systems (e.g., Bitcoin) have negative environmental impacts, i.e., the total carbon footprints of Bitcoin is 98.10 Mt CO_2 in December 2024 [161], which is comparable to the energy consumption of Qatar. A recent study [162] anticipated that these CO_2 emissions caused by PoW consensus processes expand the presence of heat-trapping greenhouse gases in Earth's atmosphere, triggering climate change and subsequent loss of property and life. Furthermore, according to the latest report from the Kaspersky security team in September 2024 [163], the number of crypto miners (e.g., Web and Windows-based miners) is still increasing; however, the most significant increase of malicious mining (or cryptojacking) [164] programs was more than 230% in 2022. They also discovered that cybercriminals utilized crypto-malware [165], which took advantage of unpatched vulnerabilities on victim devices to mine cryptocurrency (e.g., 2 Bitcoins per month based on wallets analyzed in their study). In general, consensus protocols (e.g., PoW and PoS) are proposed to prevent a specific node from controlling a blockchain or perverting the "truth" of what must be recorded by hoping to preserve the data integrity of the blockchain. In the PoW consensus mechanism, miners compete to solve convoluted mathematical puzzles as a Sybil-resistance scheme, which requires the consumption of vast electrical energy that causes a large chunk of harmful carbon footprints. By performing such complex tasks (hash rates), they verify and incorporate transactions into the public blockchain networks. Later in 2022, the Proof-of-Useful-Work (PoUW) was introduced by Hoffmann [166] as an alternative consensus algorithm involving a blockchain implemented through dedicated hardware called "node machines" with very identical, standardized properties. In this protocol, the nodes (e.g., miners) must not perform hashing processes, but rather, they produce and process blocks of transactions by deploying smart contract computations. In addition, the Network Nervous System is suggested as the core part for defining a highly secure ecosystem where the computations are run on a sovereign network of node machines as dedicated hardware. In PoUW, the repetitive hashing processes of the PoW were replaced by useful smart contract computations. PoS mechanisms encourage users to approve network data and confirm security through collateral staking. The Delegated PoS (DPoS) is a recent variant of this protocol [139], which functions differently from PoS by deploying a delegation and voting mechanism, making the verification process more democratic [29]. Instead, in the PoS, crypto owners construct blocks rather than miners; hence, they do not require particular machines that generate as many hashed values per second as possible. Consequently, the energy consumption of the PoS is negligible compared to the PoW protocol, i.e., the PoS can save approximately 99.85% of the energy currently needed to run a PoW-based system [161].

To address the negative impacts of PoW-based systems on the real-world environment, policymakers have attempted to deal with global interventions by employing fiscal and legal ways to mitigate the risks of blockchain-based systems. However, there are still unresolved issues. This is technically because Bitcoin and other PoW blockchain-based systems consume considerable energy, which can even exceed some countries' total energy consumption. For example, according to the energy consumption prediction reported by Digiconomist [161] in December 2024, the daily electrical energy consumption of the Bitcoin was estimated to be between 50 Terawatt-hour (TWh) to 204.5 TWh from March 2018 to December 2024, i.e., this is comparable to the power consumption of Poland, which is approximately 175.00 TWh (see Fig. 7). Additionally, they speculated that the CO_2 emission of one Bitcoin transaction equals the carbon footprint of 89,203 h of watching YouTube and 1,186,233 VISA payment transactions. Note that the carbon footprint of one mined Bitcoin is 597 tonnes of CO_2, almost 14.9 times more than the 140 tonnes of CO_2 needed for mining some gold worth equal to a single Bitcoin.

6.3. Cyberpsychological risks

In the modern hyper-connected IoE environments, where smart gadgets are ubiquitous, and the Internet is an inevitable part of our daily life and communication activities, a relatively new interdisciplinary field of cybersecurity and psychology has emerged to investigate the impact of cyber-related technologies on the well-being of netizens. This rather new field of study is becoming known as ***cyberpsychology***, which explores the complex correlations between netizens and cyberspace [167]. For instance, the use of GenAI tools (e.g., ChatGPT) for various applications, such as writing articles, creating creative deepfake multimedia, and crafting programming codes, is dramatically rising among netizens as a kind of human-GenAI assistant. Recent studies highlighted that GenAI tools negatively impact netizens' critical [168] and creative thinking abilities [169]. Moreover, the easy access to AI-generated content magnifies the laziness of individuals and may counteract the interest in enhancing their skills [170]. According to a recent report by the Backlinko Team in October 2024 [171], there are more than 200 million active netizens who utilize ChatGPT worldwide weekly, that was doubled compared to last year and is drastically increasing. Indeed, such ever-increasing netizens may face hallucinated GenAI-created content and then act as unintentional propagators of deepfakes, i.e., misinforming the readers by providing spurious information [172]. Below, we summarized five various forms of cyberthreats weaponized by GenAI models and LFT-QC.

– *GenAI hallucinated output:* Hallucinations happen when GenAI tools perceive objects or patterns that craft nonexistent or nonsensical

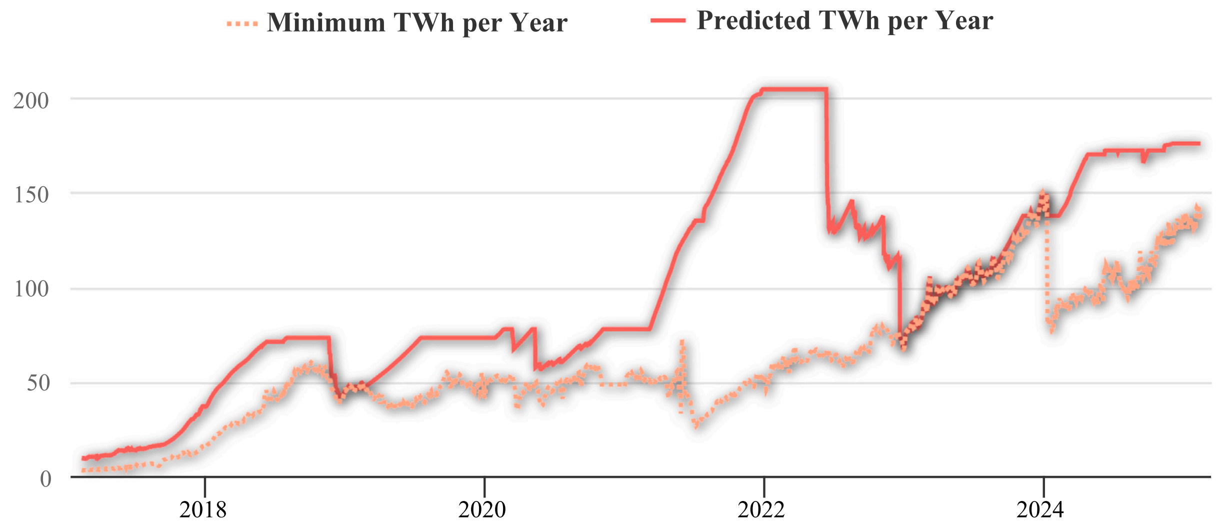


Fig. 7. A predictive analysis of annualized Bitcoin energy consumption from 12 February 2017 to 15 February 2025 [161].

outputs, which seemingly look accurate and trustworthy [173]. Sometimes, GenAI tools may even fabricate the references in the output to give the user a sense of perceived trustworthiness concerning the content's reliability. For instance, an attorney utilized the ChatGPT to do legal research to prepare a specific client's injury claim in May 2023 in New York. While reviewing the claim, the federal judge discovered that six citations mentioned in the attorney's brief were falsified [174]. In such a GenAI hallucination incident, the ChatGPT crafted imaginary references and confirmed realistically that those cases were available in major legal databases.

– ***Deepfake phishing:*** Malicious actors can deploy dark or dual-purpose GenAI tools (e.g., DarkBERT, DarkBARD, FraudGPT, WormGPT, and PoisonGPT [175]) to create hyper-targeted phishing cyber-traps, i.e., deepfake advertisements or emails by taking advantage of celebrities' reputations and their physical traits [147]. Consequently, dark GenAI tools are expected to spawn a new wave of cyber scamming schemes or offensive approaches to trick users into clicking on a link to a proxy website or installing seemingly safe software with embedded malicious codes on their devices, leading to successful account take over attacks, even with 2FA settings. In such offensive approaches, attackers deploy dark GenAI tools to craft customized phishing emails according to victims' conditions and develop malware based on recent zero-day vulnerabilities [176]. For instance, the Quantum AI Elon Musk trading bot [177] was promoted via deepfake ads through social media that is a smart investing system, which "makes you £1320 in 5 Hours and cures poverty". Indeed, unaware netizens might trust such deepfake ads and then click on the link or install the trading application, which could contain ransomware or stegomalware (e.g., GenAI-created RAT) [178].

– ***GenAI propaganda campaigns:*** Recently, malicious political parties have utilized the GenAI models to develop propaganda machines, which create deepfake news for supporting or demolishing the reputation of a particular party [179]. For instance, in January 2024, the propagation of a deepfake robocall in which President Joe Biden discouraged US citizens from voting. Later on, the USA Federal Communications Commission declared that unwanted GenAI-generated robotexts or robocalls should be prohibited by laws in February 2024 [180] and closed a comment period on public citizen's petition to legalize a new rule regarding the use of deepfakes in election advertisements.

– ***Copyright or ownership violation:*** Since the GenAI tools apply the digital replication of contents from other resources to learn and create the knowledge, they have sparked multiple class actions alleging copyright infringement [181]. It means that users are responsible for the copyright violations of GenAI-generated contents while writing prompts and confirming the results [173]. In other words, they must not only verify the ownership of GenAI-crafted contents but also their reliability must be validated; however, the outcomes could be biased because of decision-making and data-driven biases. Accordingly, many universities in the UK banned the application of GenAI tools for preparing assignments, which otherwise, it will be considered academic misconduct [182].

– ***Cyberbullying and cyberharassment:*** Cyber-offenders utilize GenAI tools to create deepfakes of underage girls or women for various nefarious purposes such as child sexual abuse, cyberstalking, and sextortion [183,184]. In a recent public alert in June 2023 [185], the Federal Bureau of Investigation (FBI) announced that they received reports on cyber-offenders applying GenAI tools to create artificial porn videos or images of underage victims. Then, they sent those deepfakes to victims to force sextortion or cyberbullying activities. To combat such unprecedented threats, the National Center for Missing and Exploited Children of the USA has developed an online system (named "Take It Down"[1]), which provides free service to help victims facing such threats to stop and prevent them.

7. Recommendations and future works

In this section, we provide strategic recommendations for policymakers, activists, and practitioners to work on the implementation challenges of PQC protocols. We also briefly describe the shortcomings of our study and suggest directions for future works, which can guide researchers in investigating the future risks of the post-quantum era.

7.1. Strategic recommendations

In the ever-changing cyberspace, there is an increasing amount of unpredictable man-made catastrophic risks that threaten the entirety of cyberspace or at least large parts of the global economy [157]. This is mainly due to the gap between regulatory, standardizing organizations, and industrial sectors that drive engines of IoE environments. As discussed above, advances in emerging technologies such as quantum AI, quantum blockchains, cryptocurrencies, and GenAI models [162] may expand the risks of cyberspace and the physical world (e.g., IoRT). Therefore, policymakers should introduce more efficient e-governance proposals [186] that could better address the ongoing and future cyberspace risks. In the following, we suggest proactive and strategic

[1] https://takeitdown.ncmec.org/

recommendations for policymakers, researchers, and practitioners to consider while confronting the following challenges:

– Standardizing organizations' evaluation metrics need to be revised significantly: The majority of current standard security protocols [20] rely upon the U2D scheme (e.g., 2FA or passwords), which is combined with the typical way of exchanging a public key and a certificate between two endpoints for performing D2D authentication approach (e.g., (D)TLS 1.2/1.3 or CoAP). Although these two protocols were standardized to protect the content of exchanged messages from being regenerated, stolen, or impersonated, they suffer from flaws, such as device dependency and reusable factors of U2D schemes as well as unencrypted certificate and weak randomness generators in (D)TLS 1.2 and 0-RTT resumption in (D)TLS 1.3. Hence, they are vulnerable to side-channel and network-based attacks [187]. A core metric behind the standardization of a protocol that might be considered is replacing classical public key protocols with dynamic multi-key fully homomorphic attribute-based encryption methods [188–190], particularly those functions based on vectors of features generated using federated learning [191] and lattice-based primitives [192], which do not only depend on complex mathematical problems. Devising side-channel protected implementations of PQC approaches with key agility [11] in security protocols must be the state of mind while engineers deploy them for D2D authentication [193]. Also, the performance of U2D schemes should be evaluated considering dynamic credentials generated based on knowledge-based factors instead of device-dependent one-time passwords (e.g., time-based 2FA) [194]. Technically, the U2D schemes should be examined based on the performance trade-offs between standard criteria such as the perceived ease-of-use, user's credentials reusability, and robustness against side-channel attacks (e.g., Downfall/Inception [8,56]) that influence users' decisions when selecting one as their security tool in real IoE environments.

– Requirements of transformative updates in blockchain consensus protocols: regulatory agencies should take proactive actions against PoW-based cryptocurrency mining farms (e.g., Bitcoin), as their negative impacts dramatically increase cyberspace energy consumption [195]. That is why the Ethereum 2.0 founders switched off the PoW and transitioned to the PoS consensus mechanism in September 2022 after merging with Beacon Chain [196]. The energy consumption-based cryptocurrency mining tax could be one way to encourage conservation and raise funds to investigate more efficient integrated chips that could be utilized in mining operations, given the potential profits from these activities. Similarly, they could impose severe legal punishments for those whose consumption is way higher than their past years' usage to motivate transformative updates in post-quantum blockchain consensus protocols (e.g., PoUW or QDPoS) and reduce environmental damage [162].

– Protecting human lives: Bitcoin is still one of the most used PoW-based cryptocurrencies in the dark web marketplaces that provides covert ways (or hard-to-trace payment methods) for malicious actors to commit cyber crimes, such as stealing digital assets via deepfake phishing schemes [197], selling firearms, and subscribing to hacking tools [198,199]. Human lives were also lost and still in danger due to the harmful emission of air pollutants caused by cryptocurrency miners on a global scale. Some recent studies [162,200] have highlighted the fact that air pollution is one of the burdens of noncommunicable diseases and mortality, which is why it was recognized as a high issue of concern by the World Health Organization. We believe that there also exists an obligatory responsibility of law enforcement agencies (e.g., the US Federal Bureau of Investigation, Interpol, Europol, and China's Ministry of Public Security) [201] to work with experts from academia, industry, and activists [202] from the United Nations Human Rights Council to form a united e-governance commission to develop security enforcement policies. These policies must comprise two components: detecting violations and taking countermeasure actions when incidents occur through cyberspace. This organization should bring together experts and strategic thinkers to define enforcement policies, introduce innovative solutions, and utilize legal or fiscal tools to reduce unprecedented threats to humanity and the environment.

– AMD Inception and Intel Downfall bugs in modern CPUs: Recently discovered vulnerabilities in modern processors have enlightened the fact that there exist unprecedented ways to bypass the security protocols from where no one could expect to emerge through hardware infrastructures [9,56], and [17]. These flaws put millions of personal and cloud computers at risk of information leakage [8]. This statement highlights the considerable gaps between standard organizations, industry, and academia, which requires more resources and investigations to build up effective and cooperative e-governance agencies in different regions (e.g., continents) where policymakers, governmental inspectors, and engineers work collaboratively to address the ongoing and future security implementation issues against cyberthreats [39].

– Cyber-wellness education (or digital media literacy) for everyone: Since the number of cyberpsychological risks of emerging technologies is on the rise, it is a significant necessity for all the netizens to get trained or be able to access free cyber-wellness educational (or digital media literacy) programs. Currently, digital media literacy programs exist in the EU[2] and other countries, such as the USA,[3] UK,[4] and Singapore,[5] which primarily are designed to train students or instructors [203]. The problem with these programs is that they exclude not only many netizens, such as elderly individuals, non-student adults, and underage netizens, but also provide limited contents that do not fully cover the necessary critical thinking knowledge and skills [204]. Therefore, upgrading, developing, and integrating effective cyber-wellness training programs must be considered the front line of governmental, educational, industrial, and media outlets, social non-profit, and educational systems to facilitate the access and outreach of necessary awareness, knowledge, and skills to all netizens [183].

7.2. Limitations and future works

In what follows, we explain the unforeseen shortcomings of our study and suggest future directions. To better elaborate our ideas, let us suppose that the LFT-QC were connected to IoE environments; thus, the following emerging problems may occur that need to be investigated in future works.

– Quantum GenAI-enabled cyberattacks: Firstly, we only focused on implementation challenges of standard PQC protocols and cyberattacks on IoE-based systems that are currently threatening cyberspace security. However, according to recent studies [205,206], we realized that the quantum GenAI models could be used to devise automated cyberattacks (e.g., Sybil [207] or DDoS [208]) to steal cryptocurrencies or turn the IoRT machines into cyberwars in the future of cyberspace. Therefore, future works can be explored by overviewing the potential adversarial risks of quantum neural networks [209] and how they are likely to be weaponized through the IoE environments.

– Legal frameworks for integration and transition to PQC protocols: Secondly, we have only suggested strategic solutions to support the transmission of classical security approaches to PQC protocols in IoE environments. However, the legal frameworks and actions could also effectively transition the implementation from classical standard security schemes to PQC protocols. Practically, the existing IoE infrastructures deploy hardware and software systems that were adapted to implement (D)TLS 1.2 and need infrastructure updates to integrate the (D)TLS 1.3, including PQC protocols [210]. Hence, future research should also consider the legal perspectives of integrating PQC protocols and how to engage and enforce the public and private sectors to accelerate the necessary infrastructure updates.

[2] https://www.digital-wellbeing.eu.

[3] https://lincs.ed.gov/.

[4] https://www.gov.uk/.

[5] https://www.moe.gov.sg/.

8. Conclusion

Authentication schemes are the front-line countermeasures for guaranteeing that an authorized user or device can access software or smart gadgets in the IoE environments. Technically, state-of-the-art solutions primarily focus on ensuring D2D authentication security, leaving the U2D authentication vulnerable to side-channel threats. On the other hand, hardware security flaws in IoE machines, such as Downfall and Inception, can provide covert channels for cyberattacks to compromise users' information.

Due to the variety of standard protocols, the need to continuously shift from one method to another in the incident of emerging cyberattacks and the necessity for compatibility of smart things and crypto-agility must be considered when developing and implementing standard security protocols. Additionally, effective cyber-wellness educational (or digital media literacy) programs must be developed and provided for all netizens to help them make informed decisions, choose safe settings, and take countermeasures when dealing with cyberspace risks.

Efforts to transform e-governance policies do not only have to rely on the NIST standard protocols, as they are limited to D2D and partially U2D authentication processes to be deployed as quantum-resistant schemes. In addition to cryptography protocols, the real-physical world needs more e-governance and enforcement policies to discover flaws and update and deploy standard schemes and cyber-wellness training programs in the real IoE environments to reduce unprecedented risks outlined in the suggested recommendations.

CRediT authorship contribution statement

Milad Taleby Ahvanooey: Investigation, Conceptualization, Methodology, Software, Data curation, Writing – original draft. **Wojciech Mazurczyk:** Investigation, Conceptualization, Writing – original draft. **Jun Zhao:** Conceptualization, Writing – original draft. **Luca Caviglione:** Discussion, Editing, Review. **Kim-Kwang Raymond Choo:** Discussion, Editing, Review. **Max Kilger:** Discussion, Editing, Review. **Mauro Conti:** Discussion, Editing, Review. **Rafael Misoczki:** Discussion, Editing, Review.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Milad Taleby Ahvanooey reports financial support was provided by National Agency for Academic Exchange. Luca Caviglione reports financial support was provided by European Union. Milad Taleby Ahvanooey reports a relationship with Warsaw University of Technology that includes: employment and funding grants. Milad Taleby Ahvanooey reports a relationship with Nanyang Technological University that includes: employment. Wojciech Mazurczyk reports a relationship with Warsaw University of Technology that includes: employment. Jun Zhao reports a relationship with Nanyang Technological University that includes: employment. Luca Caviglione reports a relationship with National Research Council of Italy that includes: employment. Kim-Kwang Raymond Choo reports a relationship with The University of Texas at San Antonio that includes: employment. Max Kilger reports a relationship with The University of Texas at San Antonio that includes: employment. Mauro Conti reports a relationship with University of Padua that includes: employment. Mauro Conti reports a relationship with Delft University of Technology that includes: employment. Rafael Misoczky reports a relationship with Meta that includes: employment. If there are other authors, they declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The study of Milad Taleby Ahvanooey was supported partially by the Ulam Research Fellowship under Grant No. BPN/ULM/2022/1/00069 funded by the NAWA-Polish National Agency for Academic Exchange in Poland and the NTU research fellowship in Singapore. The work of Luca Caviglione was supported by the Project RAISE - Robotics and AI for Socio-economic Empowerment, funded by the European Union - NextGenerationEU under Grant No. ECS00000035. The work of K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.

Data availability

No data was used for the research described in the article.

References

[1] Yirui Bai, Hong Lei, Suozai Li, Haoyu Gao, Jun Li, Leixiao Li, Decentralized and self-sovereign identity in the era of blockchain: a survey, in: 2022 IEEE International Conference on Blockchain (Blockchain), 2022, pp. 500–507.

[2] Longbing Cao, Decentralized ai: Edge intelligence and smart blockchain, metaverse, web3, and desci, IEEE Intell. Syst. 37 (3) (2022) 6–19.

[3] Aparna Kumari, Rajesh Gupta, Sudeep Tanwar, Amalgamation of blockchain and IoT for smart cities underlying 6g communication: A comprehensive review, Comput. Commun. 172 (2021) 102–118.

[4] Paul P. Momtaz, Some very simple economics of web3 and the metaverse, FinTech 1 (3) (2022) 225–234.

[5] Kelsie Nabben, Web3 as 'self-infrastructuring': The challenge is how, Big Data Soc. 10 (1) (2023) 20539517231159002.

[6] Internet of Everything (IoE), available at https://ioe.org/.

[7] Qingxuan Wang, Ding Wang, Understanding failures in security proofs of multi-factor authentication for mobile devices, IEEE Trans. Inf. Forensics Secur. 18 (2022) 597–612.

[8] Daniel Moghimi, Downfall: Exploiting speculative data gathering, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 7179–7193.

[9] AMD Team, Return address security bulletin, 2023, URL https://www.amd.com/en/resources/product-security/bulletin/amd-sb-7005.html.

[10] Wenjie Xiong, Jakub Szefer, Survey of transient execution attacks and their mitigations, ACM Comput. Surv. 54 (3) (2021) 1–36.

[11] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, Royal Hansen, Transitioning organizations to post-quantum cryptography, Nature 605 (7909) (2022) 237–243.

[12] Pengkun Li, Jinshu Su, Xiaofeng Wang, iTLS: Lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy, IEEE Internet Things J. 7 (8) (2020) 6828–6841.

[13] Dustin Moody, Angela Robinson, Cryptographic standards in the post-quantum era, IEEE Secur. Priv. 20 (6) (2022) 66–72.

[14] Milad Taleby Ahvanooey, Mark Xuefang Zhu, Qianmu Li, Wojciech Mazurczyk, Kim-Kwang Raymond Choo, Brij B Gupta, Mauro Conti, Modern authentication schemes in smartphones and IoT devices: An empirical survey, IEEE Internet Things J. (2021).

[15] NIST, CVE-2023–20583 detail, 2023, URL https://nvd.nist.gov/vuln/detail/CVE-2023-20583.

[16] NIST, CVE-2023–20569 detail, 2023, URL https://nvd.nist.gov/vuln/detail/CVE-2023-20569.

[17] NIST, CVE-2022-40982 detail, 2023, URL https://nvd.nist.gov/vuln/detail/CVE-2022-40982.

[18] First quantum computer to pack 100 qubits enters crowded race, available at : https://www.nature.com/articles/d41586-021-03476-5.

[19] Peter W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332.

[20] The beginning of the End: The first Post-Quantum- Cryptography (PQC), available at https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf.

[21] ISO Team, ISO/IEC 27001:2022, 2022, URL https://www.iso.org/.

[22] E. Rescorla, RFT:8446 - the transport layer security (TLS) protocol version 1.3, 2018, URL https://www.rfc-editor.org/rfc/rfc8446.

[23] Hamid Nejatollahi, Nikil Dutt, Sandip Ray, Francesco Regazzoni, Indranil Banerjee, Rosario Cammarota, Post-quantum lattice-based cryptography implementations: A survey, ACM Comput. Surv. 51 (6) (2019) 1–41.

[24] Qingxuan Wang, Ding Wang, Chi Cheng, Debiao He, Quantum2fa: efficient quantum-resistant two-factor authentication scheme for mobile devices, IEEE Trans. Dependable Secur. Comput. (2021).

[25] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, Rolfe Schmidt, Formal verification of the PQXDH post-quantum key agreement protocol for end-to-end secure messaging, in: 33rd USENIX Security Symposium, 2024.

[26] Wonsun Shin, May O. Lwin, Parental mediation of children's digital media use in high digital penetration countries: perspectives from Singapore and Australia, Asian J. Commun. 32 (4) (2022) 309–326.

[27] NIST Announces First Four Quantum-Resistant Cryptographic Algorithms, available at: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[28] Aykut Karakaya, Ahmet Ulu, A survey on post-quantum based approaches for edge computing security, Wiley Interdiscip. Rev.: Comput. Stat. 16 (1) (2024) e1644.

[29] Zebo Yang, Haneen Alfauri, Behrooz Farkiani, Raj Jain, Roberto Di Pietro, Aiman Erbad, A survey and comparison of post-quantum and quantum blockchains, IEEE Commun. Surv. Tutor. (2023).

[30] Hadi Gharavi, Jorge Granjal, Edmundo Monteiro, Post-quantum blockchain security for the internet of things: Survey and research directions, IEEE Commun. Surv. Tutor. (2024).

[31] Hema Shekhawat, Daya Sagar Gupta, A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era, Concurr. Comput.: Pr. Exp. (2024) e8080.

[32] Vinay Chamola, Alireza Jolfaei, Vaibhav Chanana, Prakhar Parashari, Vikas Hassija, Information security in the post-quantum era for 5G and beyond networks: Threats to existing cryptography, and post-quantum cryptography, Comput. Commun. 176 (2021) 99–118.

[33] René Mayrhofer, Stephan Sigg, Adversary models for mobile device authentication, ACM Comput. Surv. 54 (9) (2021) 1–35.

[34] Loubna Ghammam, Koray Karabina, Patrick Lacharme, Kevin Thiry-Atighehchi, A cryptanalysis of two cancelable biometric schemes based on index-of-max hashing, IEEE Trans. Inf. Forensics Secur. 15 (2020) 2869–2880.

[35] Daniel Moghimi, Berk Sunar, Thomas Eisenbarth, Nadia Heninger, {Tpm-faIL}:{tPM} meets timing and lattice attacks, in: 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 2057–2073.

[36] Milad Taleby Ahvanooey, Mark Xuefang Zhu, Wojciech Mazurczyk, Qianmu Li, Max Kilger, Kim-Kwang Raymond Choo, Mauro Conti, Covertsys: A systematic covert communication approach for providing secure end-to-end conversation via social networks, J. Inf. Secur. Appl. 71 (2022) 103368.

[37] Shanshan Li, Chunxiang Xu, Yuan Zhang, Jianying Zhou, A secure two-factor authentication scheme from password-protected hardware tokens, IEEE Trans. Inf. Forensics Secur. 17 (2022) 3525–3538.

[38] Daniel J Bernstein, Billy Bob Brumley, Ming-Shing Chen, Nicola Tuveri, {OpensslntRU}: Faster post-quantum {tLS} key exchange, in: 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 845–862.

[39] OpenSSL Team, Openssl statement on the recent intel/AMD downfall/inception vulnerabilities, 2023, URL https://openssl-library.org/post/2023-08-09-downfall/.

[40] Google Security Team, Tink cryptographic library, 2024, URL https://developers.google.com/tink.

[41] Bouncy Castle Inc., Bouncy castle – open-source cryptographic APIs, 2024, URL https://www.bouncycastle.org/.

[42] Yingchen Wang, Riccardo Paccagnella, Elizabeth Tang He, Hovav Shacham, Christopher W Fletcher, David Kohlbrenner, Hertzbleed: Turning power {side-channel} attacks into remote timing attacks on x86, in: 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 679–697.

[43] Translation: Key Chinese Think Tank2019s 201CAI Security White Paper201D (Excerpts), available at: https://digichina.stanford.edu/work/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/.

[44] Peixin Ren, Xiaozhuo Gu, Ziliang Wang, Efficient module learning with errors-based post-quantum password-authenticated key exchange, IET Inf. Secur. (2022).

[45] Catinca Mujdei, Lennert Wouters, Angshuman Karmakar, Arthur Beckers, Jose Maria Bermudo Mera, Ingrid Verbauwhede, Side-channel analysis of lattice-based post-quantum cryptography: Exploiting polynomial multiplication, ACM Trans. Embed. Comput. Syst. (2022).

[46] Ange Albertini, Thai Duong, Shay Gueron, Stefan Kölbl, Atul Luykx, Sophie Schmieg, How to abuse and fix authenticated encryption without key commitment, in: 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 3291–3308.

[47] Paul Fiterau-Brostean, Bengt Jonsson, Robert Merget, Joeri De Ruiter, Konstantinos Sagonas, Juraj Somorovsky, Analysis of {dtLS} implementations using protocol state fuzzing, in: 29th USENIX Security Symposium (USENIX Security 20), 2020, pp. 2523–2540.

[48] Liufu Zhu, Ding Wang, Robust multi-factor authentication for WSNs with dynamic password recovery, IEEE Trans. Inf. Forensics Secur. (2024).

[49] Xinyue Deng, An introduction to lenstra-lenstra-lovasz lattice basis reduction algorithm, Mass. Inst. Technol. (MIT) (2016).

[50] Cremers Cas, Garratt Luke, Smyshlyaev Stanislav V., Sullivan Nick, Wood Christopher A., Randomness improvements for security protocols (RFC 8937), 2020, URL https://datatracker.ietf.org/doc/rfc8937/.

[51] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al., Experimentally generated randomness certified by the impossibility of superluminal signals, Nature 556 (7700) (2018) 223–226.

[52] Peiying Zhang, Yaqi Wang, Gagangeet Singh Aujla, Anish Jindal, Yasser D Al-Otaibi, A blockchain-based authentication scheme and secure architecture for IoT-enabled maritime transportation systems, IEEE Trans. Intell. Transp. Syst. (2022).

[53] Pengcheng Zhao, Yuanhao Huang, Jianping Gao, Ling Xing, Honghai Wu, Huahong Ma, Federated learning-based collaborative authentication protocol for shared data in social IoV, IEEE Sensors J. 22 (7) (2022) 7385–7398.

[54] He Fang, Zhenlong Xiao, Xianbin Wang, Li Xu, Lajos Hanzo, Collaborative authentication for 6G networks: An edge intelligence based autonomous approach, IEEE Trans. Inf. Forensics Secur. 18 (2023) 2091–2103.

[55] B. Westerbaan, D. Stebila, X25519Kyber768Draft00 hybrid post-quantum key agreement, 2023, URL https://www.ietf.org/archive/id/draft-tls-westerbaan-xyber768d00-02.html.

[56] Daniël Trujillo, Johannes Wikner, Kaveh Razavi, Inception: Exposing new attack surfaces with training in transient execution, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 7303–7320.

[57] NIST, Post-quantum cryptography, 2024, URL https://csrc.nist.gov/projects/post-quantum-cryptography.

[58] Mar Gimenez-Aguilar, Jose Maria de Fuentes, Lorena Gonzalez-Manzano, Malicious uses of blockchains by malware: from the analysis to smart-zephyrus, Int. J. Inf. Secur. 22 (5) (2023) 1445–1480.

[59] Eduardo K. Viegas, Altair O. Santin, Pietro Tedeschi, Toward a reliable evaluation of machine learning schemes for network-based intrusion detection, IEEE Internet Things Mag. 6 (2) (2023) 70–75.

[60] M.E. Abdelhafez, Sureswaran Ramadass, Mustafa Abdelwahab, TLS guard for TLS 1.3 zero round-trip time (0-RTT) in a distributed environment, J. King Saud Univ.- Comput. Inf. Sci. (2023) 101797.

[61] Moritz Platt, Peter McBurney, Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance, Algorithms 16 (1) (2023) 34.

[62] Reza Azarderakhsh, Kimmo U Järvinen, Mehran Mozaffari-Kermani, Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications, IEEE Trans. Circuits Syst. I. Regul. Pap. 61 (4) (2014) 1144–1155.

[63] Jiaming Pei, Rubing Xue, Chao Liu, Lukun Wang, Towards Byzantine-resilient secure AI: A federated learning communication framework for 6G consumer electronics, IEEE Trans. Consum. Electron. (2024).

[64] Beibei Li, Peiran Wang, Zerui Shao, Ao Liu, Yukun Jiang, Yizhou Li, Defending Byzantine attacks in ensemble federated learning: A reputation-based phishing approach, Future Gener. Comput. Syst. 147 (2023) 136–148.

[65] The tls protocol version 1.0, internet engineering task force (ietf), 1999, available at: https://www.ietf.org/rfc/rfc2246.txt. (Accessed 03 April 2023).

[66] Ralph Holz, Jens Hiller, Johanna Amann, Abbas Razaghpanah, Thomas Jost, Narseo Vallina-Rodriguez, Oliver Hohlfeld, Tracking the deployment of TLS 1.3 on the web: A story of experimentation and centralization, ACM SIGCOMM Comput. Commun. Rev. 50 (3) (2020) 3–15.

[67] Xiao Lan, Jing Xu, Zhen-Feng Zhang, Wen-Tao Zhu, Investigating the multi-ciphersuite and backwards-compatibility security of the upcoming TLS 1.3, IEEE Trans. Dependable Secur. Comput. 16 (2) (2017) 272–286.

[68] E. Rescorla, Transport layer security (TLS) protocol overview, 2019, URL https://docs.oracle.com/.

[69] Hyunwoo Lee, Doowon Kim, Yonghwi Kwon, TLS 1.3 in practice: How TLS 1.3 contributes to the internet, in: Proceedings of the Web Conference 2021, 2021, pp. 70–79.

[70] Sangtae Lee, Youngjoo Shin, Junbeom Hur, Return of version downgrade attack in the era of TLS 1.3, in: Proceedings of the 16th International Conference on Emerging Networking Experiments and Technologies, 2020, pp. 157–168.

[71] Noble Kumari, A.K. Mohapatra, A comprehensive and critical analysis of TLS 1.3, J. Inf. Optim. Sci. 43 (4) (2022) 689–703.

[72] Benjamin Dowling, Marc Fischlin, Felix Günther, Douglas Stebila, A cryptographic analysis of the TLS 1.3 handshake protocol, J. Cryptology 34 (4) (2021) 37.

[73] Marcus Brinkmann, Christian Dresen, Robert Merget, Damian Poddebniak, Jens Müller, Juraj Somorovsky, Jörg Schwenk, Sebastian Schinzel, ALPACA: Application layer protocol confusion-analyzing and mitigating cracks in TLS authentication., in: USENIX Security Symposium, 2021, pp. 4293–4310.

[74] Mila Anastasova, Reza Azarderakhsh, Mehran Mozaffari Kermani, Fully hybrid TLSv1. 3 in wolfssl on cortex-M4, in: International Conference on Applied Cryptography and Network Security, Springer, 2024, pp. 376–395.

[75] Nimrod Aviram, Kai Gellert, Tibor Jager, Session resumption protocols and efficient forward security for TLS 1.3 0-RTT, J. Cryptology 34 (3) (2021) 20.

[76] Jianghong Wei, Xiaofeng Chen, Jianfeng Wang, Willy Susilo, Ilsun You, Towards secure asynchronous messaging with forward secrecy and mutual authentication, Inform. Sci. (2023).

[77] Android 10 behavior changes: all apps, 2023, available at: https://developer.android.com/about/versions/10/behavior-changes-all. (Accessed 07 April 2023).

[78] Request for comments on draft FIPS 186-5 and draft SP 800-186 (04/08/2023), available at https://www.nist.gov/news-events/news/2019/10/digital-signatures-and-elliptic-curve-cryptography-request-comments-draft.

[79] ShangMi (SM) cipher suites for TLS 1.3 (04/08/2023), available at https://datatracker.ietf.org/doc/rfc8998/.

[80] Ronaldo Serrano, Ckristian Duran, Marco Sarmiento, Cong-Kha Pham, Trong-Thuc Hoang, ChaCha20–poly1305 authenticated encryption with additional data for transport layer security 1.3, Cryptogr. 6 (2) (2022) 30.

[81] E. Rescorla, N. Modadugu, The Datagram Transport Layer Security Version 1.2 (04/08/2023), available at https://www.rfc-editor.org/rfc/rfc6347.

[82] E. Rescorla, H. Tschofenig, N. Modadugu, The Datagram Transport Layer Security (DTLS) Protocol Version 1.3 (04/08/2023), available at https://datatracker.ietf.org/doc/html/rfc9147.

[83] Y. Sheffer, P. Saint-Andre, T. Fossati, The Datagram Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) (04/08/2023), available at https://www.rfc-editor.org/rfc/rfc9325.

[84] Zane Mechalke Sullivan, Maj Bobby Birrer, Sameul Dick, Jordon Cochran, Analysis of Practical Application of Lightweight Cryptographic Algorithm ASCON Jeffrey Avery, PhD, Bryson Fraelich, William Duran, Andrew Lee, Agustin.

[85] Tschofenig Hannes, Tüxen Michael, Reddy. K Tirumaleswar, Fries Steffen, Yaroslav Rosomakho, Extended key update for transport layer security (TLS) 1.3 draft-ietf-tls-extended-key-update-03, 2024, URL https://datatracker.ietf.org/doc/draft-ietf-tls-extended-key-update/.

[86] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2 (04/14/2023), available at https://www.ietf.org/rfc/rfc5246.

[87] Daniel Owens, Rabih El Khatib, Mojtaba Bisheh-Niasar, Reza Azarderakhsh, Mehran Mozaffari Kermani, Efficient and side-channel resistant ed25519 on ARM cortex-M4, IEEE Trans. Circuits Syst. I. Regul. Pap. (2024).

[88] Kampanakis Panos, Stebila Douglas, Hansen Torben, PQ/T hybrid key exchange in SSH draft-kampanakis-curdle-ssh-pq-ke-05, 2023, URL https://datatracker.ietf.org/doc/draft-kampanakis-curdle-ssh-pq-ke/.

[89] D. Conolly, ML-KEM post-quantum key agreement for TLS 1.3, 2024, URL https://www.ietf.org/archive/id/draft-connolly-tls-mlkem-key-agreement-05.html.

[90] G. Selander, J. Mattsson, F. Palombini, L. Seitz, Object Security for Constrained RESTful Environments (OSCORE) (04/14/2023), available at https://www.rfc-editor.org/rfc/rfc8613.html.

[91] R. Housley, Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS) (04/14/2023), available at https://www.rfc-editor.org/rfc/rfc5084.

[92] H. Krawczyk, P. Eronen, HMAC-based Extract-and-Expand Key Derivation Function (HKDF) (04/14/2023), available at https://www.rfc-editor.org/rfc/rfc5869.

[93] J. Schaad, CBOR Object Signing and Encryption (COSE): Countersignatures (04/14/2023), available at https://www.rfc-editor.org/rfc/rfc9338.

[94] Phillip Harmon, Data breach notification laws and the quantum decryption problem, Wash. Lee Law Rev. 79 (1) (2022) 475.

[95] Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Xiaobo Zhou, Sang-Yoon Chang, QUIC protocol with post-quantum authentication, in: International Conference on Information Security, 2022, pp. 84–91.

[96] Rachael Shah, New study reveals what's driving—and limiting—TLS 1.3 implementation, 2022, URL https://www.f5.com/company/blog/.

[97] EMA Research Team, TLS 1.3's fourth anniversary: What have we learned about implementation and network monitoring?, 2022, URL https://www.youtube.com/watch?v=_1Y3TRs96_Y.

[98] Kimberly J Mitchell, Ateret Gewirtz-Meydan, Jennifer O'Brien, David Finkelhor, Practices and policies around wellness: insights from the internet crimes against children task force network, Front. Psychiatry 13 (2022) 931268.

[99] NIST, NIST releases first 3 finalized post-quantum encryption standards, 2024, URL https://www.nist.gov/.

[100] Elie Bursztein, Fabian Kaczmarczyck, Toward quantum resilient security keys, 2023, URL https://security.googleblog.com/2023/08/.

[101] Marissa Giustina, Bouncy castle – open-source cryptographic APIs, 2024, URL https://datatracker.ietf.org/doc/draft-ietf-tls-extended-key-update/.

[102] Davide Castelvecchi, IBM quantum computer passes calculation milestone, Nature (2023).

[103] Zebo Yang, Maede Zolanvari, Raj Jain, A survey of important issues in quantum computing and communications, IEEE Commun. Surv. Tutor. (2023).

[104] A Morvan, B Villalonga, X Mi, S Mandra, A Bengtsson, PV Klimov, Z Chen, S Hong, C Erickson, IK Drozdov, et al., Phase transition in random circuit sampling, 2023, arXiv preprint arXiv:2304.11119.

[105] Dan Garisto, Google uncovers how quantum computers can beat today's best supercomputers, Nature (2024).

[106] Rigetti Team, About rigetti computing, 2024, URL https://www.rigetti.com/about-rigetti-computing.

[107] Jeremy Kahn, D-wave took its own path in quantum computing. Now it's joining the crowd, 2021, URL https://fortune.com/2021/10/05/quantum-computer-d-wave-google-ibm-gate-model/.

[108] IonQ Team, IonQ—Trapped ion quantum computing, 2023, URL https://ionq.com/company.

[109] M Cerezo, Guillaume Verdon, Hsin-Yuan Huang, Lukasz Cincio, Patrick J Coles, Challenges and opportunities in quantum machine learning, Nat. Comput. Sci. 2 (9) (2022) 567–576.

[110] Yuan Cao, Yongli Zhao, Qin Wang, Jie Zhang, Soon Xin Ng, Lajos Hanzo, The evolution of quantum key distribution networks: On the road to the qinternet, IEEE Commun. Surv. Tutor. 24 (2) (2022) 839–894.

[111] Fazal Raheman, The future of cybersecurity in the age of quantum computers, Futur. Internet 14 (11) (2022) 335.

[112] Andrew D King, Sei Suzuki, Jack Raymond, Alex Zucca, Trevor Lanting, Fabio Altomare, Andrew J Berkley, Sara Ejtemaee, Emile Hoskinson, Shuiyuan Huang, et al., Coherent quantum annealing in a programmable 2,000 qubit ising chain, Nat. Phys. 18 (11) (2022) 1324–1328.

[113] Hongyu Wu, Xiaoning Feng, Quantum related-key differential cryptanalysis, Quantum Inf. Process. 23 (7) (2024) 269.

[114] Dedy Septono Catur Putranto, Rini Wisnu Wardhani, Harashta Tatimma Larasati, Janghyun Ji, Howon Kim, Depth-optimization of quantum cryptanalysis on binary elliptic curves, IEEE Access 11 (2023) 45083–45097.

[115] Zhonghui Li, Kaiping Xue, Jian Li, Nenghai Yu, David SL Wei, Ruidong Li, Connection-oriented and connectionless remote entanglement distribution strategies in quantum networks, IEEE Netw. 36 (6) (2022) 150–156.

[116] Liang Zhai, Giang N Nguyen, Clemens Spinnler, Julian Ritzmann, Matthias C Löbl, Andreas D Wieck, Arne Ludwig, Alisa Javadi, Richard J Warburton, Quantum interference of identical photons from remote GaAs quantum dots, Nature Nanotechnology 17 (8) (2022) 829–833.

[117] Riyaaz Uddien Shaik, Shoba Periasamy, Accuracy and processing speed trade-offs in classical and quantum svm classifier exploiting PRISMA hyperspectral imagery, Int. J. Remote Sens. 43 (15–16) (2022) 6176–6194.

[118] Amazon Team, Amazon braket, 2024, URL https://aws.amazon.com/braket/.

[119] Microsoft Team, Azure quantum cloud service, 2024, URL https://azure.microsoft.com/en-us/products/quantum/.

[120] Don Monroe, Post-quantum cryptography, Commun. ACM 66 (2) (2023) 15–17.

[121] Mario Coccia, Saeed Roshani, Melika Mosleh, Evolution of quantum computing: Theoretical and innovation management implications for emerging quantum industry, IEEE Trans. Eng. Manage. (2022).

[122] J-F Biasse, X Bonnetain, E Kirshanova, A Schrottenloher, Fang Song, Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography, IET Inf. Secur. 17 (2) (2023) 171–209.

[123] Brian Koziel, Reza Azarderakhsh, Mehran Mozaffari-Kermani, Fast hardware architectures for supersingular isogeny diffie-hellman key exchange on FPGA, in: International Conference on Cryptology in India, Springer, 2016, pp. 191–206.

[124] Srivatsan Subramanian, Mehran Mozaffari-Kermani, Reza Azarderakhsh, Mehrdad Nojoumian, Reliable hardware architectures for cryptographic block ciphers LED and HIGHT, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 36 (10) (2017) 1750–1758.

[125] Brian Koziel, Reza Azarderakhsh, Mehran Mozaffari Kermani, A high-performance and scalable hardware architecture for isogeny-based cryptography, IEEE Trans. Comput. 67 (11) (2018) 1594–1609.

[126] Yi Bian, Fangyu Zheng, Yuewu Wang, Lingguang Lei, Yuan Ma, Tian Zhou, Jiankuo Dong, Guang Fan, Jiwu Jing, AsyncGBP+: Bridging SSL/TLS and heterogeneous computing power with GPU-based providers, IEEE Trans. Comput. (2024).

[127] Brian Koziel, A-Bon Ackie, Rami El Khatib, Reza Azarderakhsh, Mehran Mozaffari Kermani, SIKE'd up: Fast hardware architectures for supersingular isogeny key encapsulation, IEEE Trans. Circuits Syst. I. Regul. Pap. 67 (12) (2020) 4842–4854.

[128] Hyeong-Gun Joo, Seunghwan Lee, Dong-Joon Shin, Extended number theoretic transform for light-weight post-quantum cryptosystems in IoT, IEEE Internet Things J. (2024).

[129] Anupama Arjun Pandit, Arun Mishra, Efficient implementation of post quantum MLWR-based PKE scheme using NTT, Comput. Electr. Eng. 118 (2024) 109358.

[130] Siavash Bayat-Sarmadi, Mehran Mozaffari-Kermani, Arash Reyhani-Masoleh, Efficient and concurrent reliable realization of the secure cryptographic SHA-3 algorithm, IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 33 (7) (2014) 1105–1109.

[131] Alvaro Cintas-Canto, Mehran Mozaffari Kermani, Reza Azarderakhsh, Error detection constructions for ITA finite field inversions over gf on FPGA using CRC and hamming codes, IEEE Trans. Reliab. 72 (2) (2022) 651–661.

[132] Mojtaba Bisheh-Niasar, Reza Azarderakhsh, Mehran Mozaffari-Kermani, High-speed NTT-based polynomial multiplication accelerator for post-quantum cryptography, in: 2021 IEEE 28th Symposium on Computer Arithmetic, ARITH, IEEE, 2021, pp. 94–101.

[133] Mehran Mozaffari Kermani, Amir Jalali, Reza Azarderakhsh, Lightweight error detection architectures through swapping the shares for a subset of S-boxes, in: 2018 IEEE 61st International Midwest Symposium on Circuits and Systems, MWSCAS, IEEE, 2018, pp. 578–581.

[134] Mojtaba Bisheh Niasar, Reza Azarderakhsh, Mehran Mozaffari Kermani, Optimized architectures for elliptic curve cryptography over curve448, Cryptol. EPrint Arch. (2020).

[135] Rami Elkhatib, Brian Koziel, Reza Azarderakhsh, Mehran Mozaffari Kermani, Cryptographic engineering a fast and efficient SIKE in FPGA, ACM Trans. Embed. Comput. Syst. 23 (2) (2024) 1–25.

[136] Jipeng Zhang, Junhao Huang, Lirui Zhao, Donglong Chen, Çetin Kaya Koç, ENG25519: Faster TLS 1.3 handshake using optimized X25519 and Ed25519, in: Usenix Security, 2024.

[137] Minrui Xu, Xiaoxu Ren, Dusit Niyato, Jiawen Kang, Chao Qiu, Zehui Xiong, Xiaofei Wang, Victor CM Leung, When quantum information technologies meet blockchain in web 3.0, IEEE Netw. 38 (2) (2023) 255–263.

[138] Maximus Liu, Khadijeh Najafi, Michael Dubrovsky, Mikhail Y Shalaginov, Cryptocurrency mining with quantum computers, in: Quantum 2.0, Optica Publishing Group, 2023, pp. QTu3A–2.

[139] Qin Li, Jiajie Wu, Junyu Quan, Jinjing Shi, Shichao Zhang, Efficient quantum blockchain with a consensus mechanism qdpos, IEEE Trans. Inf. Forensics Secur. 17 (2022) 3264–3276.

[140] Statista, Total value of cryptocurrency lost to and recovered from theft and other attacks between march 2020 and february 2022, 2023, URL https://www.statista.com/statistics/1285057/crypto-theft-size/.

[141] Statista, Value of e-commerce losses to online payment fraud worldwide from 2020 to 2023, 2023, URL https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/.

[142] Chainalysis Team, 2024 crypto crime trends: Illicit activity down as scamming and stolen funds fall, but ransomware and darknet markets see growth, 2024, URL https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/.

[143] TRM's threat intelligence team, Thefts from crypto hacks and exploits surge in first half of 2024, 2024, URL https://www.trmlabs.com/.

[144] Immunebytes Team, List of compromised private key crypto hacks, 2024, URL https://www.immunebytes.com/blog/list-of-compromised-private-key-crypto-hacks/.

[145] Jun Zhang, Dan Tenney, The evolution of integrated advance persistent threat and its defense solutions: A literature review, Open J. Bus. Manag. 12 (1) (2023) 293–338.

[146] Luca Caviglione, Wojciech Mazurczyk, Never mind the malware, here's the stegomalware, IEEE Secur. Priv. 20 (5) (2022) 101–106.

[147] Mekhail Mustak, Joni Salminen, Matti Mäntymäki, Arafat Rahman, Yogesh K Dwivedi, Deepfakes: Deceptions, mitigations, and opportunities, J. Bus. Res. 154 (2023) 113368.

[148] Kaspersky Team, Kaspersky discovers 'tusk,' active information and crypto stealing campaign, 2024, URL https://www.kaspersky.com/.

[149] Abdulrahman Alamer, Sultan Basudan, Security and privacy of network transmitted system in the internet of robotic things, J. Supercomput. (2022) 1–18.

[150] Madalina Popovici, ShellBot ddos malware targets poorly managed linux servers, 2023, URL https://heimdalsecurity.com/.

[151] Truc Nguyen, My T. Thai, Denial-of-service vulnerability of hash-based transaction sharding: Attack and countermeasure, IEEE Trans. Comput. (2022).

[152] Sundaram Mishra, Shivam Mishra, Yan Chi Toh, Satyam Mishra, Phung Thao Vi, Mitigating the threat of multi-factor authentication (MFA) bypass through man-in-the-middle attacks using EvilGinx2, Creative Approaches Towar. Dev. Comput. Multidiscip. IT Solut. Soc. (2024) 59–78.

[153] Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf.

[154] Mauro Conti, E. Sandeep Kumar, Chhagan Lal, Sushmita Ruj, A survey on security and privacy issues of bitcoin, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3416–3452.

[155] Christian Leuprecht, Caitlyn Jenkins, Rhianna Hamilton, Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency, J. Financ. Crime 30 (4) (2023) 1036–1054.

[156] Savino Dambra, Leyla Bilge, Davide Balzarotti, A comparison of systemic and systematic risks of malware encounters in consumer and enterprise environments, ACM Trans. Priv. Secur. (2021).

[157] Interpol, Financial and cybercrimes top global police concerns, says new interpol report, 2022, URL https://scamcryptorobots.com/quantum-ai-review-scam/.

[158] VLAD CONSTANTINESCU, New 'address poisoning' crypto scam on the rise, metamask warnsl, 2023, URL https://nvd.nist.gov/vuln/detail/CVE-2023-20583.

[159] Huntley Shane, Nagy Luca, Disrupting the glupteba operation, 2021, URL https://blog.google/threat-analysis-group/disrupting-glupteba-operation/.

[160] Check Point Team, June 2024's most wanted malware, 2024, URL https://blog.checkpoint.com/.

[161] Digiconomist, Bitcoin energy consumption index, 2024, URL https://digiconomist.net/bitcoin-energy-consumption.

[162] Jon Truby, Rafael Dean Brown, Andrew Dahdal, Imad Ibrahim, Blockchain, climate damage, and death: Policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and bitcoin, Energy Res. Soc. Sci. 88 (2022) 102499.

[163] Kaspersky Team, Threat landscape for industrial automation systems. Q2 2024, 2024, URL https://ics-cert.kaspersky.com/publications/reports/2024/.

[164] Aggeliki Tsohou, Vasiliki Diamantopoulou, Stefanos Gritzalis, Costas Lambrinoudakis, Cyber insurance: state of the art, trends and future directions, Int. J. Inf. Secur. (2023) 1–12.

[165] Janaka Senanayake, Harsha Kalutarage, Mhd Omar Al-Kadri, Andrei Petrovski, Luca Piras, Android source code vulnerability detection: a systematic literature review, ACM Comput. Surv. 55 (9) (2023) 1–37.

[166] Felix Hoffmann, Challenges of proof-of-useful-work (pouw), in: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & beyond (IGETblockchain), IEEE, 2022, pp. 1–5.

[167] Marshall S. Rich, Cyberpsychology: A longitudinal analysis of cyber adversarial tactics and techniques, Anal. 2 (3) (2023) 618–655.

[168] Michael Agyemang Adarkwah, GenAI-Infused adult learning in the digital era: A conceptual framework for higher education, Adult Learn. (2024) 10451595241271161.

[169] Abdullahi Yusuf, Shamsudeen Bello, Nasrin Pervin, Abdullahi Kadage Tukur, Implementing a proposed framework for enhancing critical thinking skills in synthesizing AI-generated texts, Think. Ski. Creat. 53 (2024) 101619.

[170] Lynsey Meakin, Exploring the impact of generative artificial intelligence on higher education students' utilization of library resources: A critical examination, Inf. Technol. Libr. 43 (3) (2024).

[171] Backlinko Team, ChatGPT / openai statistics: How many people use ChatGPT? 2024, URL https://backlinko.com/chatgpt-stats.

[172] David Uriel Socol de la Osa, Nydia Remolina, Artificial intelligence at the bench: Legal and ethical challenges of informing—or misinforming—judicial decision-making through generative AI, Data Policy 6 (2024) e59.

[173] Jeandri Robertson, Caitlin Ferreira, Elsamari Botha, Kim Oosthuizen, Game changers: A generative AI prompt protocol to enhance human-ai knowledge co-construction, Bus. Horiz. (2024).

[174] Ramishah Maruf, Lawyer apologizes for fake court citations from ChatGPT, 2023, URL https://edition.cnn.com/2023/05/27/business/chat-gpt-avianca-mata-lawyers/index.html.

[175] Abdul-Fatawu Abdulai, Is generative AI increasing the risk for technology-mediated trauma among vulnerable populations? Nurs. Inquiry 32 (1) (2025) e12686.

[176] Araz Taeihagh, Governance of generative AI, 2025.

[177] Stephan Lindburg, Quantum AI review, fake quantum AI SCAM by elon musk exposed!, 2024, URL https://scamcryptorobots.com/quantum-ai-review-scam/.

[178] Samuel Greengard, Hidden malware ratchets up cybersecurity risks, Commun. ACM 65 (10) (2022) 16–18.

[179] Jelena Cupać, Mitja Sienknecht, Regulate against the machine: how the EU mitigates AI harm to democracy, Democr. (2024) 1–24.

[180] Federal Communications Commission, Implications of artificial intelligence technologies on protecting consumers from unwanted robocalls and robotexts, 2024, URL https://www.federalregister.gov/.

[181] Uri Y. Hacohen, Niva Elkin-Koren, Copyright regenerated: Harnessing genai to measure originality and copyright scope, Harv. J. Law Technol. 37 (2) (2024).

[182] Tom Burnett, Cambridge university among elite universities to ban ChatGPT due to plagiarism fears, 2023, URL https://www.cambridge-news.co.uk/.

[183] Milad Taleby Ahvanooey, Wojciech Mazurczyk, Dongwon Lee, Socio-economic threats of deepfakes and the role of cyber-wellness education in defense, Commun. ACM 68 (1) (2025) 1–8.

[184] Marie-Helen Maras, Kenji Logie, Countering the complex, multifaceted nature of nude and sexually explicit deepfakes: an Augean task? Crime Sci. 13 (1) (2024) 1–17.

[185] FBI Field Office, Malicious actors manipulating photos and videos to create explicit content and sextortion schemes, 2024, URL https://www.ic3.gov/Media/Y2023/PSA230605/.

[186] Gaby Umbach, Igor Tkalec, Evaluating e-governance through e-government: Practices and challenges of assessing the digitalisation of public governmental services, Eval. Program Plan. 93 (2022) 102118.

[187] Using early data in http, internet engineering task force (ietf), 2018, available at: https://www.rfc-editor.org/rfc/rfc8470. (Accessed 19 March 2023).

[188] Yuling Chen, Sen Dong, Tao Li, Yilei Wang, Huiyu Zhou, Dynamic multi-key FHE in asymmetric key setting from LWE, IEEE Trans. Inf. Forensics Secur. 16 (2021) 5239–5249.

[189] Marco Rasori, Michele La Manna, Pericle Perazzo, Gianluca Dini, A survey on attribute-based encryption schemes suitable for the internet of things, IEEE Internet Things J. 9 (11) (2022) 8269–8290.

[190] Yisong Wang, Jun Zhou, Zhenfu Cao, Xiaolei Dong, Kim-Kwang Raymond Choo, Mueoc: Efficient SGX-based multi-key homomorphic outsourcing computation for E-health system, IEEE Trans. Dependable Secur. Comput. (2024).

[191] Fan Yang, Yanan Qiao, Mohammad Zoynul Abedin, Cheng Huang, Privacy-preserved credit data sharing integrating blockchain and federated learning for industrial 4.0, IEEE Trans. Ind. Inform. 18 (12) (2022) 8755–8764.

[192] Iván Blanco-Chacón, Alberto Pedrouzo-Ulloa, Rahinatou Y Njah Nchiwo, Beatriz Barbero-Lucas, Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields, Cryptogr. Commun. (2025) 1–35.

[193] Markku-Juhani O. Saarinen, WiP: Applicability of ISO standard side-channel leakage tests to NIST post-quantum cryptography, in: 2022 IEEE International Symposium on Hardware Oriented Security and Trust, 2022, pp. 69–72.

[194] Conor Gilsenan, Fuzail Shakir, Noura Alomar, Serge Egelman, Security and privacy failures in popular {2FA} apps, in: 32nd USENIX Security Symposium (USENIX Security 23), 2023, pp. 2079–2096.

[195] Jinsong Zhan, Shaofeng Dong, Wei Hu, Ioe-supported smart logistics network communication with optimization and security, Sustain. Energy Technol. Assess. 52 (2022) 102052.

[196] Oliver J. Hall, Stavros Shiaeles, Fudong Li, A study of ethereum's transition from proof-of-work to proof-of-stake in preventing smart contracts criminal activities, Netw. 4 (1) (2024) 33–47.

[197] Yisroel Mirsky, Wenke Lee, The creation and detection of deepfakes: A survey, ACM Comput. Surv. 54 (1) (2021) 1–41.

[198] Yogesh K Dwivedi, Laurie Hughes, Abdullah M Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M Al-Debei, Denis Dennehy, Bhimaraya Metri, Dimitrios Buhalis, Christy MK Cheung, et al., Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, Int. J. Inf. Manage. 66 (2022) 102542.

[199] Yuntao Wang, Zhou Su, Ning Zhang, Rui Xing, Dongxiao Liu, Tom H Luan, Xuemin Shen, A survey on metaverse: Fundamentals, security, and privacy, IEEE Commun. Surv. Tutor. (2023).

[200] Shali Tayebi, Heresh Amini, The flip side of the coin: Exploring the environmental and health impacts of proof-of-work cryptocurrency mining, Environ. Res. (2024) 118798.

[201] Milad Taleby Ahvanooey, Mark Xuefang Zhu, Wojciech Mazurczyk, Max Kilger, Kim-Kwang Raymond Choo, Do dark web and cryptocurrencies empower cybercriminals, in: 12th EAI International Conference on Digital Forensics & Cyber Crime, EAI ICDF2C 2021, Singapore, 2021.

[202] Francis M. Idzi, Ricardo Corrêa Gomes, Digital governance: government strategies that impact public services, Glob. Public Policy Gov. (2022) 1–26.

[203] Yancy Toh, Chee-Kit Looi, Transcending the dualities in digital education: A case study of Singapore, Front. Digit. Educ. 1 (2) (2024) 121–131.

[204] Liisa Ilomäki, Minna Lakkala, Veera Kallunki, Darren Mundy, Marc Romero, Teresa Romeu, Anastasia Gouseti, Critical digital literacies at school level: A systematic review, Rev. Educ. 11 (3) (2023) e3425.

[205] Carlos A Riofrio, Oliver Mitevski, Caitlin Jones, Florian Krellner, Aleksandar Vuckovic, Joseph Doetsch, Johannes Klepsch, Thomas Ehmer, Andre Luckow, A characterization of quantum generative models, ACM Trans. Quantum Comput. 5 (2) (2024) 1–34.

[206] Xiaodong Ding, Qibing Xiong, Jinchen Xu, Fudong Liu, Junling Qiu, Yu Zhu, Yifan Hou, Zheng Shan, Intelligent generative models for quantum neural networks, Adv. Quantum Technol. 2400178.

[207] Chenhan Zhang, Shui Yu, Zhiyi Tian, James J.Q. Yu, Generative adversarial networks: A survey on attack and defense perspective, ACM Comput. Surv. 56 (4) (2023) 1–35.

[208] Francesco Musumeci, Ali Can Fidanci, Francesco Paolucci, Filippo Cugini, Massimo Tornatore, Machine-learning-enabled ddos attacks detection in p4 programmable networks, J. Netw. Syst. Manage. 30 (2022) 1–27.

[209] Jinkai Tian, Xiaoyu Sun, Yuxuan Du, Shanshan Zhao, Qing Liu, Kaining Zhang, Wei Yi, Wanrong Huang, Chaoyue Wang, Xingyao Wu, et al., Recent advances for quantum neural networks in generative learning, IEEE Trans. Pattern Anal. Mach. Intell. 45 (10) (2023) 12321–12340.

[210] Abdullah Aydeger, Engin Zeydan, Awaneesh Kumar Yadav, Kasun T Hemachandra, Madhusanka Liyanage, Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography, in: 2024 15th International Conference on Network of the Future (NoF), IEEE, 2024, pp. 195–203.