Security Journal (2024) 37:1640–1679
https://doi.org/10.1057/s41284-024-00435-3

ORIGINAL ARTICLE

Digital security by design

Petar Radanliev[1,2]

Accepted: 31 May 2024 / Published online: 19 June 2024

Abstract

This paper scrutinises the evolving digital security landscape, encompassing technological advancements, regulatory frameworks, and industry-specific challenges. It explores the influence of technologies like AI, quantum computing, and blockchain on security paradigms whilst identifying emergent threats. The study analyses the interplay between digital security and legislative policies, underlining their impact on industry practices and individual behaviours. Sector-specific examinations are conducted, pinpointing unique security concerns in sectors such as healthcare and finance and advocating bespoke solutions. The study highlights discrepancies between security intentions and actions, proposing strategies to bridge this divide. Projecting into the future, we anticipate shifts in technology and regulation, culminating in pragmatic recommendations for stakeholders. This article offers an informed perspective on digital security, laying the groundwork for proactive approaches in a dynamic digital environment.

Keywords Emerging technologies · Sector-specific security concerns · Regulatory frameworks · Digital security · Technological advancements · Regulatory frameworks · Perception–action gap

Introduction

The digital environment has become the centre of modern society (Cao 2021; ENISA 2023b; Roumani et al. 2016), and as it expands, the need to strengthen its security has never been more pressing. This in-depth examination of the digital security landscape exposes a complex interplay of emerging technologies, ranging from the duality of quantum computing's potential weaknesses (Diamanti et al. 2016) to the resilience provided by AI-driven defences (ENISA 2023a; Mishra 2023). Along with these technological complexities, the regulatory environment is racing to adapt

✉ Petar Radanliev
petar.radanliev@cs.ox.ac.uk

[1] Department of Computer Science, University of Oxford, Oxford, UK

[2] School of Management, University of Bath, Bath, UK

(Bommasani et al. 2023; European Parliament 2023; FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation That Protects Americans' Rights and Safety | The White House 2023; Mozumder et al. 2022), dealing with the vastness of international cyber threats, assuring the appropriate evolution of emerging technologies, and establishing data protection regulations. Furthermore, exploring sector-specific concerns, ranging from healthcare to manufacturing, emphasises the need for personalised digital security solutions to address industrial challenges. Compounding these difficulties is the problem of defining and implementing the genuine benefit of digital security, bridging the apparent gap between stakeholders' objectives and behaviours. Looking ahead, we see a mash-up of predicted threats, transformational technological advances, and mutable regulatory contours. The study results with suggestions for a unified, proactive posture, pushing stakeholders to integrate technology, policy, and ethical behaviour to shape a secure digital future.

Definition and scope of digital security

Digital security, cybersecurity, or information technology security are the strategies and methods to protect information, devices, networks, programmes, and data from cyberattacks, damage, or unauthorised access. Regardless of the definition, the primary objective of digital security is to establish a safe environment for transactions, communications, data processing, and storage.

Contrarily, information security protects data integrity and confidentiality in storage or transit. The scope of digital security is broad and includes many different elements. By preventing unauthorised access, misuse, or alteration of computer networks and network-accessible resources, network security, for instance, aims to preserve the integrity and usability of networks, data, and resources. Another crucial aspect of digital security is application security, which focuses on keeping devices and software safe from attackers. The data that an application is supposed to protect may be accessible to attackers if it is compromised.

Operational security, computer network, and application security are other essential components of the digital security infrastructure. It includes the policies governing how and where data may be stored or transferred and the processes and choices necessary to administer and protect data assets, such as individual users' access rights to company networks.

Business continuity planning and catastrophe recovery are included in the scope of digital security. This topic focuses on developing plans to guarantee that an organisation can resume regular operations following a security incident. These strategies include restoring the data's availability, integrity, and privacy. End-user education is another essential component of digital security. Users may unintentionally introduce viruses into their systems and harm the network without any fault of their own. As a result, a crucial component of any effective digital security strategy is educating consumers about potential dangers and best practices.

The security of Internet of Things (IoT) devices is a digital security concern (Jalali et al. 2019; Tanczer et al. 2018). These devices are frequently a source of network security vulnerability, making them a favourite target for attackers. The field of technology known as “IoT security” (Abie and Balasingham 2012; Ahmad and Alsmadi 2021; Altman Vilandrie & Company, 2017; Ani et al. 2019; Ayad et al. 2019; Brass et al. 2018; Crawford and Sherman 2018; Ghirardello et al. 2018; Jalali et al. 2019; Latvala et al. 2020; Payton 2018; Roopak et al. 2019; Russell and Van Duren 2016) is devoted to protecting the networks and linked devices that comprise the IoT ecosystem. Finally, the security of cloud-based platforms is crucial as data continue to move there. Cloud security combines rules, controls, procedures, and technology to protect cloud-based systems.

The purpose and importance of digital security in 2024

Given the growing number of digital dangers, the need for reliable digital security measures is becoming increasingly evident. Digital security becomes crucial for businesses, governments, and individuals as more personal information is kept and shared online. Besides traditional information security, digital security by design also connects with crime science and situational crime prevention. For example, the concept of ‘Situational Crime Prevention’ (Clarke 1997) refers to ‘an analysis of the circumstances giving rise to specific kinds of crime’ and recommends a set of criteria ‘to reduce the opportunity for those crimes to occur’. (Clarke 1997), with a focus on crime reduction (Wortley et al. 2018). In this review, we found that some literature connects ‘technology and crime’ (Ekblom 2017), and we wanted to expand upon this area by investigating the new concepts of security by design and security by default.

In 2024, as our reliance on technology grows, cybersecurity and digital security will become even more essential in safeguarding data integrity, confidentiality, and availability. One of the critical issues with digital security is that we need to have undisturbed operations whilst defending information systems, including devices, networks, and programmes, from cyber threats, including malware, hacking, and phishing. The operational perspective is applicable in a wide range of areas, including network, information, and application security, as well as in developing industries like the Internet of Things (IoT) and cloud computing.

Another significant design conflict identified in the study is the juxtaposition of convenience versus security within the IoT and cloud computing. As the digital landscape gravitates towards increased interconnectivity and user-centric designs, a critical tension emerges between ensuring user convenience and maintaining robust security protocols. On the one hand, IoT devices and cloud platforms are designed for ease of use, accessibility, and seamless integration into daily activities, which often necessitates a certain level of openness and data sharing. On the other hand, this very openness poses substantial security risks, making these systems vulnerable to cyberattacks and data breaches. This contradiction becomes even more pronounced with the advent of technologies like 5G and AI, which further enhance connectivity but also expand the potential attack surface. Thus, the challenge for designers lies in striking an optimal balance: developing user-friendly, efficient systems fortified with advanced security measures to counteract emerging cyber threats. This design conflict embodies the quintessential struggle in digital security by design—the need to harmonise user experience with stringent security requirements (Bhingarkar et al. 2022; Botta et al. 2016; Cavalcante et al. 2016; Cook and Van Horn 2011; de Bruin and Floridi 2017; Díaz et al. 2016; ENISA 2009; Sehgal et al. 2020; Sparks et al. 2015; Sunyaev 2020; Wan et al. 2014; Xu et al. 2019b).

Digital security protects personal information from cybercrimes such as identity theft, financial fraud, and privacy violations. When digital security is coordinated with organisations' operational strategies, it maintains the firm's operational integrity and economic stability, lowering the danger of data breaches that could result in significant financial and reputational harm.

Looking at the bigger picture, digital security also protects critical infrastructures from cyberattacks that could threaten national security on a large scale. Many cyberattacks on critical infrastructure are designed to use vulnerabilities in personal devices or company digital infrastructures. In the IoT, big data and artificial intelligence age, digital security governs the safe and ethical application of new technologies, preventing unauthorised use and misuse of devices and data.

Current state of digital security in 2024

In 2024, digital security has evolved to become more complicated and sophisticated, reflecting the rapid advancement of technology. Advanced defensive techniques are emerging due to the exponential growth of emerging technologies like 5G, AI, and IoT, which have significantly increased the possible attack surface for malevolent groups.

We can see a shift from the conventional perimeter-based security design towards a zero-trust security architecture at the network level. Zero-trust networks enforce tight identity verification for every person and device trying to access network resources, regardless of where they are located, presuming that possible threats could originate inside and outside the network.

Security solutions are now more fully integrating artificial intelligence and machine learning (Mishra 2023; Porambage et al. 2019). By evaluating trends, anticipating potential attacks, and automating responses, these technologies improve the ability to recognise and respond to threats. They also present new difficulties since threat actors use these technologies to plan more complex attacks.

The sharp rise in linked devices presents particular security difficulties on the IoT front (Tanczer et al. 2018). Although IoT devices provide efficiency and convenience, their scale, heterogeneity, and typically laxer security requirements create several exploitable vulnerabilities.

Hybrid and multi-cloud techniques are becoming more widely used and pose new security challenges as the cloud domain develops. Whilst cloud providers provide some security features, it is up to enterprises to protect their data on the cloud, which calls for cloud-native security solutions (Akinrolabu et al. 2019; Sehgal et al. 2020).

Cybersecurity talent is still a concern. As the complexity and number of threats rise, there is an urgent demand for competent cybersecurity personnel to handle these attacks. More complex training is being developed, and efforts are being made to entice more people to work in the field.

What will define digital security in 2024 is a difficult balance between adopting transformational technologies and managing unique cyber threats. This dynamic environment highlights the need for constant review and improvement in digital security practices, technologies, and policies.

The emergence of the digital domain as a central pillar of contemporary society has underscored the significance of comprehensive digital security. With our ever-growing dependency on digital infrastructures, a deep understanding of the countless parts of digital security is crucial. For this reason, the study aims and objectives are designed to undertake a broad-ranging review of the field in this study.

Aims of the review

As digital domains enter every area of our lives, keeping up with digital security improvements and difficulties is critical. This review study aims to provide stakeholders with an up-to-date and compact reference, allowing informed judgments and pre-emptive steps in the face of an ever-changing digital security scenario.

This urgency is compounded by the evolving nature of threats (as seen in Fig. 1), rapid technological advancements, changing regulatory environments, and sector-specific challenges.

Objective

The primary objective of this rapid study is to provide a concise yet thorough overview of the present digital security landscape. The review structure is explained and can be described as specifically designed to

1. Explore the Technological Landscape: Examine the most recent advancements and difficulties in digital security technologies, ranging from encryption approaches to the significance of new domains like artificial intelligence, quantum computing, and blockchain in changing security paradigms.
2. Examine the Regulatory Framework: The current legal and policy framework connected to digital security focuses on the interplay between national and international legislation and its overarching impact on industries and individual behaviours.
3. Examine Sectoral Implications: Investigate the distinct digital security concerns and considerations that exist in several industries, with a focus on healthcare, banking, retail, manufacturing, and the public sector. Recognising the unique

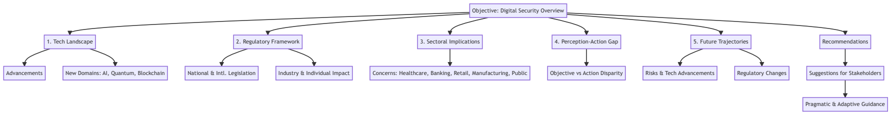

Objective: Digital Security Overview
1. Tech Landscape
2. Regulatory Framework
3. Sectoral Implications
4. Perception-Action Gap
5. Future Trajectories
Recommendations
Advancements
New Domains: AI, Quantum, Blockchain
National & Intl. Legislation
Industry & Individual Impact
Concerns: Healthcare, Banking, Retail, Manufacturing, Public
Objective vs Action Disparity
Risks & Tech Advancements
Regulatory Changes
Suggestions for Stakeholders
Pragmatic & Adaptive Guidance

Fig. 1 Aims and objectives of the research study

nature of challenges and solutions for each industry is critical for comprehensive knowledge.

4. Assess the Perception–Action Gap: Investigate the reoccurring theme of the disparity between digital security objectives and real-world actions to understand the causes of this gap and potential solutions.
5. Anticipate Future Trajectories: Forecast what changes are probable in the digital security ecosystem, such as growing risks and problems, technology advancements, and altering regulatory paradigms.

The recommendations expected from the review consist of actionable suggestions for diverse stakeholders, ranging from individual users to global politicians, based on the synthesised findings whilst ensuring that the guidance is pragmatic, forward-thinking, and adaptive. Across various sectors, universal digital security challenges such as data encryption, identity management, and zero-trust architectures are consistently vital. These challenges underscore the overarching need for data integrity and privacy protection. Core principles like confidentiality and integrity are crucial across industries, whether in healthcare, finance, or retail. The persistent threat of cyberattacks like phishing and ransomware demands a unified approach to cybersecurity, blending sector-specific solutions with general principles to safeguard the digital ecosystem.

Bibliometric review

Before building the methodology, we conducted a bibliometric analysis of data records on the Web of Science Core Collection. We chose the Web of Science Core Collection because it includes a variety of indexes, such as

- Science Citation Index Expanded (SCIE) (Coverage:1965-present)
- Social Sciences Citation Index (SSCI) (Coverage:1965-present)
- Arts & Humanities Citation Index (AHCI) (Coverage:1975-present)
- Book Citation Index (BKCI) (Coverage: 2005-present)
- Conference Proceedings Citation Index (CPCI) (Coverage:1990-present)
- Emerging Sources Citation Index (ESCI) (Coverage: 2017-present)

Another reason we chose the Web of Science Core Collection is because it represents more than 21,000 peer-reviewed, high-quality scholarly journals published worldwide in over 250 sciences, social sciences, and arts & humanities disciplines, as well as conference proceedings and book data.

The first search was conducted on ‘Digital Security by Design’, producing 8157 results. We wanted to determine the research areas for these records. We used a statistical analysis approach based on the 8157 results and the VOSviewer (Jan van Eck and Waltman 2009), the R Studio (Aria and Cuccurullo 2017), and the Web of Science Analyse Results tool. Then, in this review, we tested the validity of the data with a combination of workshops and face-value thematic

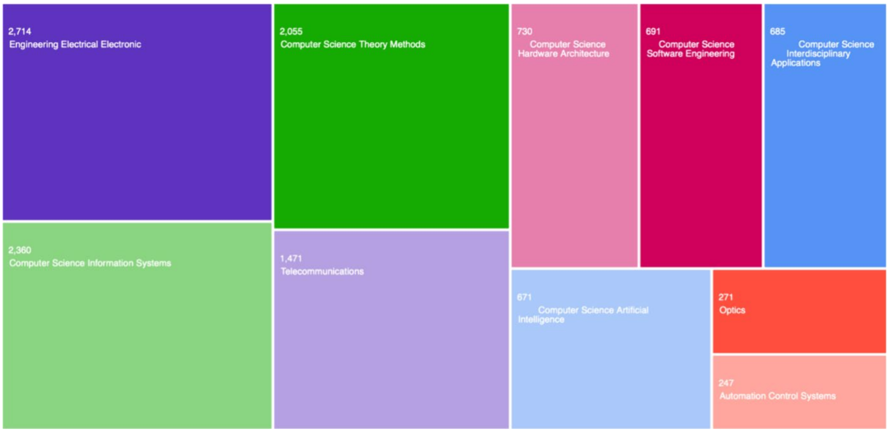


Fig. 2 Digital security by design categories of research areas

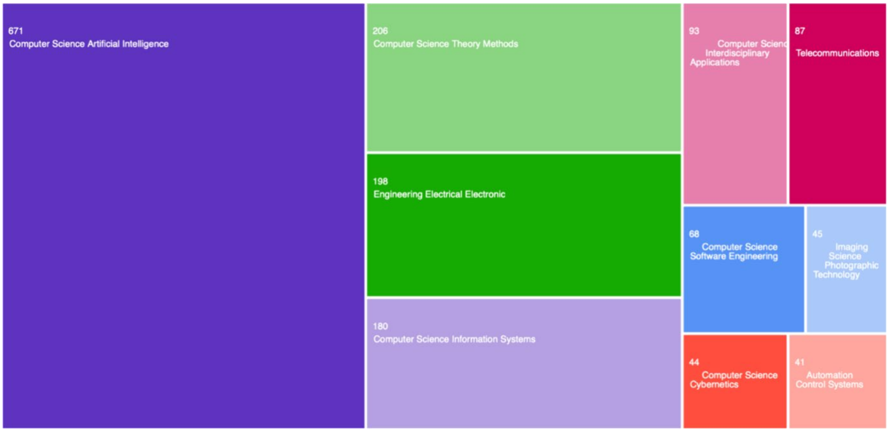


Fig. 3 Digital security by design and artificial intelligence

analysis. The records are categorised by the number of publications in a specific category to determine the areas. From this, we can visualise the emerging categories in Fig. 2.

The visualisation in Fig. 2 shows that most of the research conducted in 'Digital Security by Design' is in computer science and engineering science. To narrow the focus, given the recent advancements in Generative AI, we decided to analyse data records specific to Computer Science Artificial Intelligence. In this category, we found a total of 671 records. We categorised these records again in Fig. 3.

Although the categorisations in Fig. 3 are somewhat interesting, we could not determine the specific research areas related to these categories. The study used R statistical programming to investigate these data further with the bibliometrics bibliophily plugin (Aria and Cuccurullo 2017).

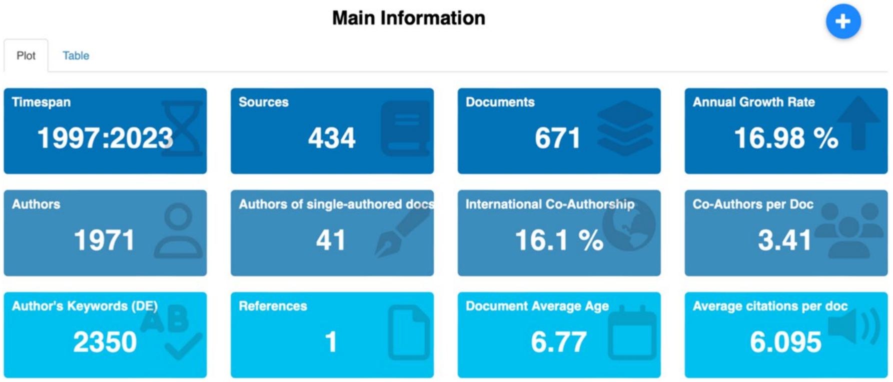
Biblioshiny presented a different view of the primary information. In Fig. 4, we can see the timespan of the data records from 1997 to 2023. We can also see that most records result from collaborative work, and only 41 single-authored data records are in the data file.

Figure 4 is included to increase the visibility of how the data were selected for this study and ensure other researchers can reproduce the study. Although the categories in Fig. 4 can seem very abstract and unrelated to content issues, the information is included to enable other researchers to reproduce the study in the future. This information can be seen as the 'Bill of Materials' of the data sources used in this study's analysis, including the data collection period. The contribution of Fig. 4 is not to show the findings in themselves but to show transparency of the intermediate stage in the analysis process.

The following visualisation we produced was a Three-Field Plot, and we wanted to determine the most productive authors and then categorise authors by countries and affiliations. The results are a lot more interesting than we expected. The data showed a strong dominance of Chinese authors and affiliations. We will make this file publicly available for other researchers to test and reproduce the results. But even without the data file, we have detailed the process for obtaining this data file, and anyone can produce the same file by following the same search parameters on the Web of Science Core Collection. What interested us mainly was why Chinese authors and affiliations predominate this area of research when most of the new commercial contributions in artificial intelligence, such as ChatGPT, Bart, etc., are all in the US.

In the subsequent visualisation, using the same dataset as in Fig. 5, we wanted to determine what keywords are used in these records. In other words, we tried identifying the aims and objectives that predominated this dataset.

In Fig. 6, we can visualise the clustering by coupling, where emerging categories originate from the keywords, global citation score, and title terms. Those are categorised with N-Grams into Unigrams. The number of units is 250, the minimum cluster frequency is 5, the label per cluster is 3, and the label size is 0.3.



Main Information

Timespan 1997:2023

Sources 434

Documents 671

Annual Growth Rate 16.98 %

Authors 1971

Authors of single-authored docs 41

International Co-Authorship 16.1 %

Co-Authors per Doc 3.41

Author's Keywords (DE) 2350

References 1

Document Average Age 6.77

Average citations per doc 6.095

Fig. 4 Main information analysis with bibliometrics

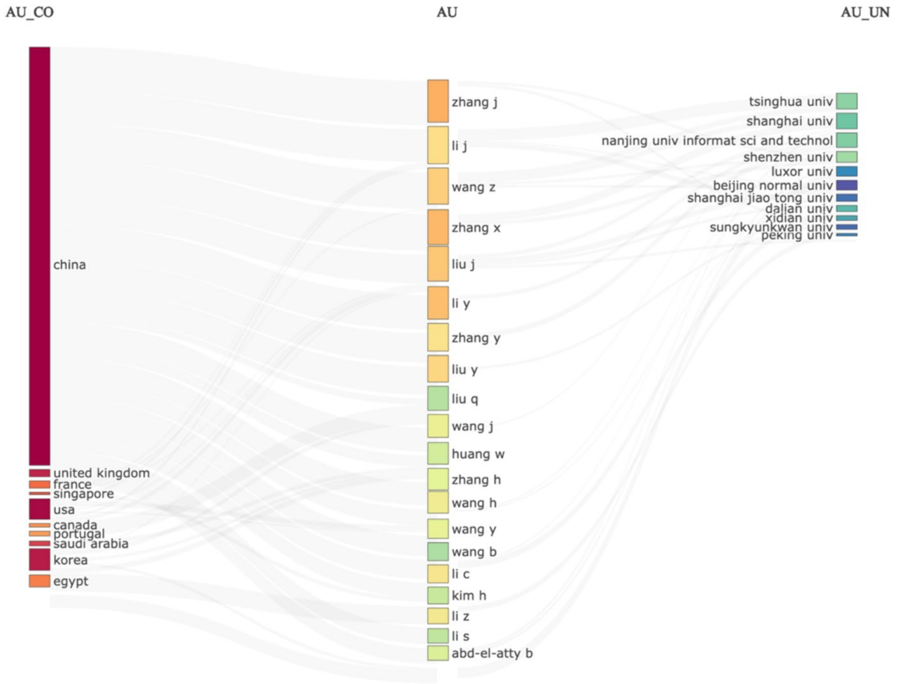


Fig. 5 Three-field plot of countries, authors, and universities

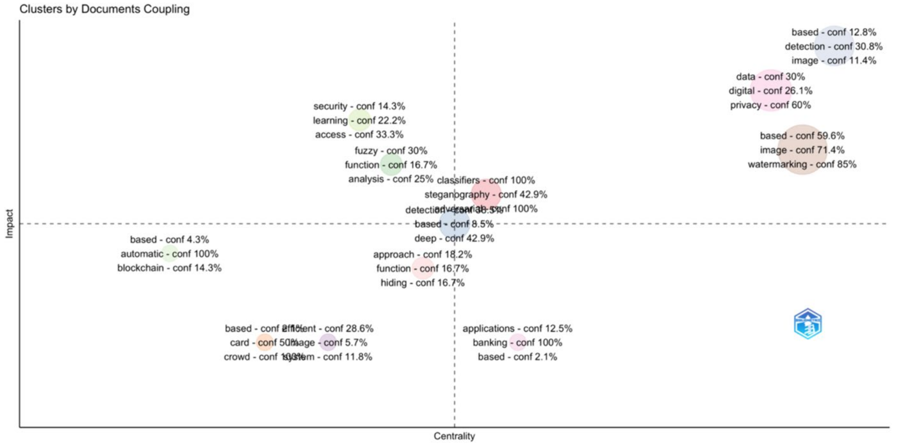


Fig. 6 Clustering by coupling of keywords used in the data records analysed

To explain what the N-grams and Unigrams mean in the context of the **biblioshiny** plugin of the **bibliometrix** package in R, which is used to produce. N-grams and Unigrams are integral to text analysis and data mining, and in Fig. 6, these concepts refer to

(a) **Unigrams**: A unigram is a single word or term. In text analysis, a unigram approach means that each word is treated as a separate entity. In the context of **bibliophily, when analysing bibliometric data (like titles, abstracts,** and keywords of academic papers), unigrams refer to the individual words extracted from these texts. Unigram analysis is often used to identify the most frequently occurring words in a dataset, which can indicate the main topics or themes in a collection of academic literature.

(b) **N-Grams**: An N-gram is a contiguous sequence of 'n' items from a given sample of text or speech. The 'n' can be any integer. For instance, a 2-g (or bigram) is a two-word sequence (like "machine learning"), and a 3-g (or trigram) is a three-word sequence (like "natural language processing"). In **biblioshiny**, N-grams are used to identify and analyse sequences of words that frequently occur together in the bibliometric data. This is more informative than unigrams because N-grams can capture more context. For example, whilst unigrams might identify 'artificial' and 'intelligence' as frequent terms, a bigram analysis would identify the phrase 'artificial intelligence'. N-gram analysis in bibliometrics is particularly useful for uncovering common themes, research trends, and patterns in scientific literature.

Understanding the distribution and frequency of unigrams and N-grams in a dataset can provide valuable insights into the key focus areas of research, emerging trends, and the evolution of topics over time in a given field. This is particularly relevant in cybersecurity, artificial intelligence, and blockchain technology, as analysing these terms can reveal significant patterns and shifts in research focus within these domains.

The **conf** is an abbreviation for 'confidence', commonly used in statistical contexts. The clustering presented in Fig. 6 refers to the confidence level of specific assignments or predictions (in this case, the 95% confidence interval). In other words, it represents the confidence score that a data point belongs to a particular cluster. The second abbreviation that seems slightly confusing is **based**. This is part of a variable name in a function. In Fig. 6, **based** is part of a naming convention for variables or parameters, indicating the basis or foundation of the calculation. In other words, the 'distance-based' refers to the distance metrics for forming clusters. More specifically, in this study, **based** derives from the relevant bigrams and refers to the trending topic based on the author's keywords.

After this analysis, it became clear that we needed to expand into a more qualitative approach for the study. The Chinese authors and institutions predominate the Web of Science Core Collection data records, representing the scientific publications in this research area. We wanted to investigate if the other areas of 'Digital Security by Design' also represent the same regional powers. To compare the statistical analysis, we started with a review of frameworks and industry-produced literature. This approach is detailed in the methodology chapter.

Methodology

The methodology used in this review of the current uses of "Digital Security by Design" (Ani et al. 2020; Ayad et al. 2019; CISA 2023; Craggs and Rashid 2017; Nawir et al. 2016; Radanliev et al. 2018) in 2024 is based on a review of existing frameworks, literature selected, and systematic analysis. This study intends to provide a clear overview of the "Digital Security by Design" situation in 2024 through a precise review structure, careful literature selection, and an exhaustive review procedure.

Review framework

The research methodology is based on a thematic analytical technique specially tailored for analysing different components of "Digital Security by Design". This method was chosen because it enables the discovery, evaluation, and reporting of patterns in the chosen literature. The themes were carefully selected based on their recurrence in the literature and applicability to the study's central question, "The current state of Digital Security by Design".

Selection of literature

The literature was chosen from various sources, including journal papers, case studies, and other online sources. These resources include ScienceDirect, IEEE Xplore, and Google Scholar. The selection procedure was governed by predetermined criteria, such as the publishing date (post-2020), the article's applicability to the topic, its peer-reviewed status, and the use of English. We rejected papers that lacked empirical support or did not directly address "Digital Security by Design".

Review procedure

The review started with examining the abstracts following the predetermined criteria. The shortlisted literature was then thoroughly read and analysed. Using a thematic analytical technique, each item of literature was evaluated with an emphasis on identifying significant themes and supporting subthemes that provide a new understanding of "Digital Security by Design" from the period between 2020/24. Extracted information was focussed on the 'Digital Security by Design' sector's new trends, problems, and prospective future orientations. The reading and analytical phases of this review procedure were repeated to gather all relevant data. Two research approaches, qualitative and quantitative, are used to separately complete each stage of the evaluation process, reducing potential biases or oversight to improve the reliability and validity of the results. As the first step in developing conclusions using this method, the study presents the core principles of 'Digital Security by Design' in a sequence diagram (Fig. 7) to ensure a solid and perceptive description of digital security.

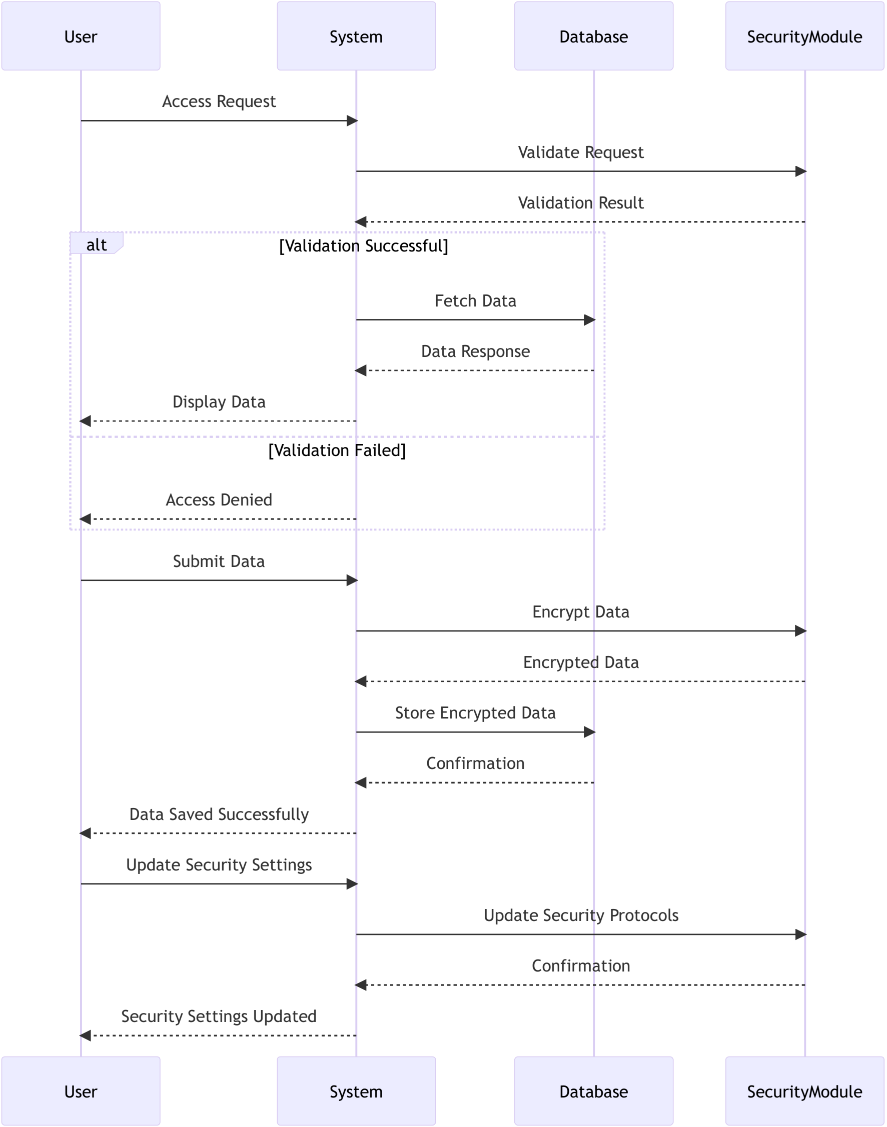


Fig. 7 Digital security by design—sequence diagram

The sequence diagram in Fig. 7 illustrates the interactions between a user, a system, a database, and a security module in a “Digital Security by Design” framework. When a user requests access, the system initially consults the security module to validate the request. If validated, the system retrieves data from the database for the user. When the user submits data, the system directs the security module to encrypt it before storing it in the database. Additionally, users can update security settings, prompting the system to adjust security protocols via the security module, ensuring a dynamic and secure environment. The following section reviews the core principles for providing a dynamic and secure environment.

Core principles of digital security

Confidentiality

In 2024, increased security is achieved through sophisticated encryption techniques, such as homomorphic encryption, which enables calculations on encrypted data, and quantum encryption, which uses the laws of quantum mechanics. Businesses have embraced zero-trust architectures, which by default prevent data disclosure unless access is specifically authorised, in response to the global implementation of tighter data protection rules, such as the revised General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) (CCPA 2018).

Integrity

In 2024, maintaining data reliability and consistency in the face of sophisticated cyber threats will constitute integrity. Blockchain technology, for example, has a wide range of uses in this context. Data integrity is upheld via blockchain's immutable ledger technology, guaranteeing data consistency and offering a clear audit trail of data updates. Advanced intrusion detection systems (IDS) (Anthi et al. 2019; Sultana et al. 2019; Vinayakumar et al. 2019), which watch systems for malicious activity or policy breaches to stop unauthorised data tampering, have also been developed due to the rise of AI.

In 2024, new regulations, including the EU Cybersecurity Act (ENISA 2023b), will impose strict requirements for data integrity. To further ensure data integrity, these legal frameworks underline the importance of certification programmes for ICT goods, services, and processes.

Accessibility

Scalable and durable systems like cloud and edge computing will guarantee availability in 2024. These innovations reduce the likelihood of system outages whilst providing on-demand access to data and services. Furthermore, they provide quick system failovers and redundant data instances, which promote effective disaster recovery and business continuity planning. In cloud and edge computing, failovers are automated processes that enable a system to rapidly switch to a backup system in case of failure, ensuring minimal downtime. This mechanism is crucial for maintaining high availability, particularly in scalable and durable systems, where the goal is continuous access to data and services. Failovers support effective disaster recovery and business continuity by providing quick recovery options and reducing the impact of system outages. The use of geographical redundancy in cloud computing and local processing in edge computing enhances this capability, ensuring that even in the event of significant disruptions, such as technical failures or natural disasters, the system remains operational with minimal disruption to services.

The year 2024 will see the development of new cyber-resilience strategies, such as using autonomous systems that use AI to foresee and avert future system disruptions. Such systems automatically adjust to network demands, ensuring that services are always available. The minimal security requirements for IoT devices are governed by policies like the Internet of Things Cybersecurity Improvement Act in the US, which significantly improves system availability. According to the Act, IoT suppliers must provide their products with sufficient security features to ensure system reliability and avoid any availability disruptions by compromised IoT devices.

Valuation of digital security

Valuation in this context refers to determining digital security's monetary worth or importance within various domains—individual, organisational, and national. It involves quantifying the potential financial impact of cybersecurity threats and the cost-effectiveness of investments in cybersecurity measures. Methods vary from risk-based calculations like Annualised Loss Expectancy at the individual level to strategic models like the Gordon–Loeb Model for organisational investment and extend to national assessments that weigh the severity of cyber threats against the necessary investment in digital security infrastructure. The goal of valuation in digital security is to optimally allocate resources to protect against cyber threats whilst considering economic efficiency and the broader impact on the entity involved.

Individual valuation methods

At the individual level, risk-based methodologies are regularly used to quantify the value of digital security. Such methods are designed to estimate and forecast the possible loss from a cybersecurity attack. One technique, the Annualised Loss Expectancy (ALE), calculates the potential annual loss from risk by dividing the Single Loss Expectancy (SLE) by the Annualised Rate of Occurrence (ARO). People will also rely on more sophisticated AI-powered tools in 2024 to simulate different attack scenarios, calculate the economic impact, and hone their security investment strategies.

The Gordon–Loeb Organisation investment model

The Gordon–Loeb Model (Gordon and Loeb 2002) is still a popular strategy for directing cybersecurity spending at the organisational level. According to this concept, the ideal sum to invest in cybersecurity should be at most 37% of the anticipated damage brought on by a security breach. By 2024, businesses had modified this model to account for new dangers brought on by cutting-edge technologies like 5G and AI, and they had adjusted their security budgets to reflect the possible risk and harm brought on by security breaches in these fields.

A national assessment based on perceived threats

The value placed on digital security at the national level is correlated with the perceived severity of the cyber threat. Typically, nations that perceive threats as serious make more significant investments in cyber security. Starting in 2024, we can expect governments to use AI-powered threat intelligence platforms to identify and quantify potential risks in real time, enabling a more precise assessment of digital security. With the development of comprehensive national cybersecurity programmes, countries have started considering the possible social effects of cyberattacks, such as the interruption of crucial infrastructure, in their valuation methodologies.

Factors affecting digital security practices

Individual factors: PMT and SDT

According to the Protection Motivation Theory (PMT) (Rogers 1975), people evaluate their reactions to threats based on the risks, perceived risk severity, susceptibility, effectiveness, and self-efficacy. Recent studies in 2024 operationalised these constructs in the context of cyber risks. For instance, dangers from advanced persistent threats (APTs), ransomware, and social engineering assaults are now included in the definition of perceived susceptibility.

The Self-Determination Theory (SDT) (Ryan and Deci 2000, 2017) strongly emphasises how autonomy, competence, and relatedness influence people's decision to engage in specific actions. SDT has been used to explain the adoption of safe behaviours like routine software updates, two-factor authentication, and virtual private networks (VPNs) in the context of digital security in 2024. Platforms for customised learning powered by AI have been crucial in promoting competency in these areas, which supports adopting safe behaviour.

Organisational factors: cultural competence, economic incentives, and psychological ownership

Employee attitudes towards safeguarding information assets are influenced by psychological ownership within firms. As remote labour becomes more prevalent in 2024, it is imperative to guarantee psychological ownership of digital assets. Businesses have implemented tactics like ongoing engagement, open communication, and establishing an inclusive atmosphere.

In 2024, the significance of corporate culture to digital security has increased. Businesses have adopted comprehensive cybersecurity frameworks that align with their corporate cultures. For instance, several firms have included the NIST Cybersecurity Framework in their organisational cultures, which encompasses identifying, protecting, detecting, responding, and recovering.

Economic incentives are effective strategies companies use to promote digital security practices. Businesses use blockchain-based smart contracts (Azzi et al. 2019; Bajoudah et al. 2019; Chamola et al. 2020; Chang and Park 2020; Chanson et al. 2019; Cheikhrouhou et al. 2022; Deshmukh et al. 2022; Dong et al. 2018; Faqir-Rhazoui et al. 2021; Feng et al. 2022; Hajizadeh et al. 2023; Hazra et al. 2022; He et al. 2022; Ishmaev 2019; Javaid et al. 2020; Kumar et al. 2020; Lawrenz et al. 2019; Liu et al. 2021; Lucio et al. 2022; Mahmood et al. 2022; Mogavero et al. 2021; Mozumder et al. 2022; Nguyen and Ali 2019; Prakash et al. 2022; Ranganthan et al. 2018; Sachdev 2019; Schlatt et al. 2023; Sittón-Candanedo 2020; Wylde et al. 2022; Xu et al. 2019a, 2022) to implement performance-based incentives transparently and effectively, paying staff for adhering to cybersecurity best practices and meeting security goals. Employee engagement in cybersecurity behaviours has increased, thanks to integrating these incentive systems with gamified cybersecurity training platforms.

Current threats and vulnerabilities

Awareness of risks and empowerment

Understanding cybersecurity risks is crucial in 2024 for reducing threats and vulnerabilities. Cyber threats such as Advanced Persistent Threats (APTs), ransomware, phishing, and IoT-based attacks are becoming more sophisticated. One of the new strategies is training people and organisations to understand these risks and how to counter them.

AI-powered platforms identify and quantify possible risks in real time, enabling quick reaction and mitigation. Organisations have also embraced sophisticated Machine Learning and AI algorithms for predictive analytics, helping them anticipate and prepare for future cyber threats based on patterns and trends in data.

Psychological ownership of data

An individual's perception of possessiveness and control over personal or organisational data is called psychological ownership of data. Individuals' attitudes and behaviours towards data protection are influenced by their psychological convictions.

Promoting data ownership has become essential in 2024 as cyber risks increase. Strategies like data anonymisation and pseudonymisation have been used, supported by laws like the GDPR (GDPR 2018; ICO 2018) and CCPA. Organisations have also developed transparent data handling procedures and privacy-by-design strategies to strengthen psychological ownership and foster trust.

Changing digital security culture

In 2024, organisations are shifting their security strategies to be more proactive than reactive. This calls for ongoing threat detection, frequent security reviews, and adopting a "zero-trust" philosophy. Real-time threat identification and response are made possible by the increasing usage of technologies like AI and machine learning for security automation and orchestration. To foster a culture of security, employee training programmes have switched their emphasis from simple awareness to behavioural change, using techniques like gamification and continuous feedback. The increased C-suite involvement in cybersecurity issues indicates a recognition of cyber risk as a strategic business risk. This is another indicator of the change in the culture around digital security. As a result, rather than being considered a separate activity, cybersecurity is now an essential component of organisational culture.

Security technologies and solutions

Encryption technologies

Technology-based encryption is essential for protecting digital communication and data. Widely used symmetric encryption uses the same key for encryption and decoding. The Advanced Encryption Standard (AES) (NIST 2001), frequently used, is well known for its attack resilience. AES serves as the security foundation for many security systems. On the other hand, asymmetric encryption uses two keys: a public key for encryption and a private key for decryption. This contrast makes secure communication possible, with the RSA algorithm (Rivest et al. 1978) being a common technique. Encryption is frequently used in digital signatures and is crucial for safe online transactions and private communications (Zhang et al. 2018). Encryption, which safeguards data integrity and confidentiality, remains an essential defence line as cyber threats change.

Network security solutions

Data's integrity, confidentiality, and availability as it transfers across networks are protected by various technologies and approaches under the overarching framework of network security. Firewalls operate as barriers, controlling traffic and implementing security regulations. Even the most advanced and modern firewalls fail to detect all cyber vulnerabilities. To address this, we use penetration testing to identify undetected vulnerabilities in modern firewalls. The importance of intrusion detection systems (IDS) (Anthi et al. 2018, 2019; Sultana et al. 2019; Vinayakumar et al. 2019; Yin et al. 2019) and intrusion prevention systems (IPS) has also increased. IDS notices suspicious activity, whereas IPS actively blocks possible threats.

In contrast, virtual private networks (VPNs) encrypt tunnels they build to protect data in transit. When working remotely, VPNs are essential for preventing data theft and eavesdropping. Network security solutions are a complicated and dynamic field that continuously adapts to new security threats and evolving network architectures.

Endpoint security

Endpoint security protects individual access points such as computers and mobile devices. This involves constantly scanning for vulnerabilities using antivirus and anti-malware software. Heuristic analysis is used in modern variants of these technologies to understand the behaviour of unknown threats. Endpoint detection and response (EDR) solutions keep track of all endpoint activity and collect data for in-depth analysis. EDR enables rapid response to threats and uncovers potential weaknesses. Another critical feature is Mobile Device Management (MDM), which controls and secures access to corporate data on mobile devices. With the development of different endpoint devices in the corporate landscape, ensuring security across all these points has become a complicated but critical task.

Cloud security

The adoption of cloud computing has resulted in new security paradigms. This required a new approach to cybersecurity. Cloud security extends traditional security concepts into a distributed, virtualised setting. Access to cloud services, for example, is governed by Identity and Access Management (IAM) systems. IAM enables multi-factor authentication and single sign-on features to ensure that only authorised users can access specific resources. Cloud Access Security Brokers (CASBs) function as middlemen, enforcing security policies across a wide range of cloud services. Data encryption, both at rest and in transit, is vital to cloud security. This tiered security technique creates a robust barrier against data breaches and unauthorised access in cloud environments.

Artificial intelligence and machine learning in security

Artificial Intelligence (AI) and machine learning (ML) have become critical components of modern security measures. Predictive analysis, in which AI can analyse large data sets to forecast future risks, enables preventative interventions. Machine learning algorithms can be trained to recognise ‘normal’ patterns and discover anomalies that indicate risks. These technologies improve human capacities by delivering insights that might otherwise go unnoticed. AI-powered automated response systems also respond faster to attacks, decreasing possible damage. AI and ML are not without obstacles, such as biases in training data, but their continuing progress and inclusion into security policies have the potential to transform how security is handled.

Blockchain for digital security

Blockchain's use in digital security goes beyond what we got accustomed to with media coverage on cryptocurrency. Blockchain immutability preserves data integrity, making any change traceable because modifications require consensus across all ledger copies. This technology has applications in supply chain tracking, healthcare data management, and many other fields. Another breakthrough is smart contracts, which are self-executing contracts with terms integrated into code. This ensures that agreed-upon agreements are followed without intermediaries, hence expediting operations. Blockchain-enabled decentralised identity management can give individuals more control over their data, lowering the danger of identity theft. In a world plagued by data breaches and fraud, blockchain's transparent yet secure nature provides novel answers to some of the most critical security issues.

Policies and regulations

Policies and regulations: steering the digital security landscape

Policies and laws are the cornerstones that assure a balance between innovation, privacy, and security in our modern digital era. These notions serve as solid foundations, guiding best practices and digital behaviours. These legal and regulatory frameworks can be challenging, but understanding them is critical for organisations or individuals to function in the digital environment.

Current legal framework for digital security

Today's legal framework for digital security consists of long-standing rules adapted for the digital age and new regulations formed in response to developing risks. Cybersecurity legislation primarily focuses on three main areas: infrastructure protection, data security, and cybercriminal prosecution. The combination of international treaties and domestic regulations creates a multi-layered defence against various threats.

Digital security regulations in many jurisdictions compel organisations to implement proper security measures to protect consumer data and maintain business continuity. Failure to satisfy these criteria can result in significant penalties, including financial and reputational damages. The regulatory framework also includes cybercrime, providing authorities with the tools they need to prosecute those who participate in malicious cyber operations. This framework continually evolves to reflect the digital world's dynamic nature.

National and international regulations

Although national legislation handles issues inside specific borders, the interconnected nature of the digital world requires international collaboration.

Countries have established regulatory organisations and frameworks adapted to their dangers and weaknesses. For example, the UK's National Cyber Security Centre (NCSC) [81] provides standards, resources, and incident response capabilities to safeguard the country's digital assets.

However, cyber threats frequently cross boundaries, demanding international cooperation. Organisations such as the International Telecommunication Union (ITU) and Interpol provide a venue for governments to share intelligence, agree on best practices, and combat global cyber threats collaboratively. Furthermore, conventions like the Budapest Convention on Cybercrime (Council of Europe 2001) encourage international collaboration in prosecuting cybercriminals by overcoming potential gaps in national legislation.

Privacy laws and their impact on digital security

Privacy has become a significant concern in the digital age, with many people considering it a fundamental human right. This mentality has resulted in a flood of privacy-related legislation and regulations worldwide. The General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States are notable examples. These rules give individuals control over their data and require organisations to collect, use, and secure it.

In addressing the implications of privacy laws on digital security, it is critical to acknowledge the potential for their exploitation by malevolent actors. Regulations like the GDPR and CCPA, whilst empowering individuals with control over their data, inadvertently engender a quandary in digital security. This dilemma manifests as a design conflict: augmenting legitimate users' privacy whilst limiting criminal misuse opportunities. The resolution of this paradox necessitates a sophisticated, balanced approach. It requires the development of advanced identity verification and data tracking mechanisms that respect privacy yet are adept at discerning and thwarting illicit activities. Policymakers and technologists must collaboratively ensure that privacy regulations are not static bastions but dynamic systems capable of differentiating between legitimate privacy needs and their exploitation by offenders. Thus, privacy laws can contribute positively to the digital security landscape, bolstering trust and safety without inadvertently facilitating cybercrime.

The role of incentivisation

Incorporating the concept of incentivisation within policies and regulations could act as a pivotal policy lever in steering the digital security landscape. This approach aligns well with the framework of mobilisation of preventers (5Is 2002), emphasising various stakeholders, including individuals and organisations, to actively participate in crime prevention. In this context, the concept of 'supercontrollers' (Sampson et al. 2010) is particularly relevant. Supercontrollers are entities or mechanisms that can influence or control the actions of potential offenders, guardians, or managers in a way that prevents crime, including cybercrime. This concept can be applied to digital security, where policies and regulations can act as super controllers by incentivising organisations to adopt robust cybersecurity measures, thus preventing cyber threats. Incentivising adherence to privacy laws, such as the GDPR and the CCPA, through rewards or the avoidance of penalties can also encourage organisations to prioritise digital security. By integrating these concepts into the legal framework for digital security, policymakers can create a more proactive, preventative approach to cybersecurity, thereby reinforcing the multi-layered defence against various threats and balancing the intricate relationship between privacy, security, and innovation.

These privacy laws have a significant impact on digital security. Whilst they primarily address privacy rights, the need to secure personal data highlights the importance of solid digital security measures. Companies must increasingly preserve client data for moral, business, and legal reasons. Under these standards, inadequate security that results in data breaches can result in significant fines, not to mention reputational damage. Also, the difficulty of balancing data accessibility for legitimate objectives with privacy and security has resulted in advancements in data processing and storage. Data anonymisation techniques are now widely used to erase or transform identifiable information. Similarly, end-to-end encryption is becoming more common as businesses strive to secure data privacy in transit and at rest.

Digital security in different sectors

Digital security in different sectors: tailoring strategies for diverse challenges

The structure of our current digital ecosystem is interlaced with a multitude of sectors, each with its own set of security concerns and complexities. The security paradigm transforms as industries undergo digital transformation, necessitating industry-specific techniques. The section below presents a short perspective of the changing digital security landscape across industries.

Health care

As a sector at the intersection of life-saving therapies and cutting-edge technology, health care is particularly sensitive to digital security problems. Electronic Health Records (EHRs) (Miotto et al. 2016), telemedicine platforms, and connected medical equipment have increased because of the digital transformation in health care. Whilst these advancements improve patient care, they also create new vulnerabilities. Patient data integrity and confidentiality are critical. Breach violates privacy rules, such as the Health Insurance Portability and Accountability Act (HIPAA) (1996) in the United States and can also be fatal. For example, a cyberattack that modifies prescription data can have disastrous consequences. Furthermore, ransomware assaults on hospitals have underlined the importance of robust security mechanisms. With patient lives on the line, these institutions are frequently excellent targets for hostile actors looking to take advantage of the critical requirement for system functionality.

Finance

The financial sector has been a focus point for digital security measures for many years. It is no wonder that banks and financial organisations confront sophisticated attacks, given the sensitive nature of economic data and the monetary incentives for cybercriminals. Threats range from Distributed Denial of Service (DDoS) attacks (Rajakumaran et al. 2020) to interrupt services to phishing efforts to confuse customers. As a result, the sector has implemented strict security measures. Multi-factor authentication, encrypted communications, and sophisticated fraud detection algorithms are already industry standards. The development of fintech has contributed to the digital financial tapestry, prompting collaborations between incumbent banks and start-ups to create a cohesive security policy.

Retail

The retail industry's embrace of e-commerce and digital platforms has transformed shopping experiences whilst introducing new cyberattack vectors. With an increasing frequency of online transactions, protecting payment information is critical. Credit card data breaches can destroy customer trust and result in hefty financial fines. Furthermore, with the introduction of the Internet of Things (IoT), even physical establishments are incorporating digital solutions, ranging from intelligent shelves to connected point-of-sale systems. Because each connecting point represents a potential vulnerability, merchants must implement comprehensive cybersecurity plans that span both their physical and digital worlds.

Manufacturing

With the transformation to Industry 4.0 (Bär et al. 2018; Bécue et al. 2021; Caiado et al. 2021; Dalenogare et al. 2018; Faller and Feldmüller 2015; Fatorachian and Kazemi 2021; Ghodmare et al. 2021; Gunasekaran et al. 2018; Hamid 2022; Hofmann and Rüsch 2017; Jazdi 2014; Kolberg and Zühlke 2015; Lee et al. 2014, 2015; Lezzi et al. 2018; Liao et al. 2017; Ministry of Economy Industry and Competitiveness Accessibility 2015; Müller et al. 2018; Pan et al. 2015; Peasley et al. 2017; Peukert et al. 2020; Radanliev 2019; Radanliev et al. 2021; Reischauer 2018; Rinaldi et al. 2019; Rivas et al. 2018; Schlechtendahl et al. 2014; Shao et al. 2021; Sittón-Candanedo 2020; Sokolov and Ivanov 2015; Stock and Seliger 2016; Sung 2017; Waslo et al. 2017; Weyer et al. 2015), the industrial industry is integrating digital technologies on an unprecedented scale. Intelligent factories with networked machinery, automated processes, and data-driven decision-making exemplify this change. However, the digital network that drives efficiency also poses security risks. Cyber-physical attacks, in which digital breaches have physical implications, are particularly concerning. An intrusion that disrupts a manufacturing line or changes product requirements might affect supply chains, product quality, and safety. As manufacturing facilities become more digital, a strong security posture protecting data and physical processes is critical.

Public sector

Government enterprises and public sector organisations are burdened with providing necessary services whilst protecting citizen data. From e-governance platforms to brilliant city efforts, digital transformations in this sector aim to improve efficiency and public involvement. However, digital security is a primary focus because of the sensitive nature of government data and the possible societal impact of disruptions. Cyber espionage, hacktivism, and cyber warfare are particularly relevant challenges to the public sector. Protecting critical infrastructure such as power grids, transportation systems, and communication networks necessitates a multi-layered security strategy capable of detecting, mitigating, and responding to various attacks.

Research and knowledge gaps

Research and knowledge gaps: illuminating the obscurities in digital security

Maintaining a proactive position in the continuously changing field of digital security is critical. Understanding present knowledge gaps helps drive future research endeavours and guarantees that preventive measures remain effective as new dangers emerge and technologies advance. This chapter digs into some of the less-explored areas of digital security, finding topics that merit additional examination.

Defining/measuring value of digital security

Determining the financial value of digital security remains a challenging task. The benefits, such as preventing cyberattacks and protecting data integrity, are apparent. However, measuring these benefits in financial or other quantitative terms can be elusive. Furthermore, because security is preventative, its worth is somewhat subjective; how can we quantify an occurrence that was avoided and the consequent avoided damages? There is an apparent demand for comprehensive measurements and frameworks that can provide a complete picture of the value obtained from digital security. The research goal should be to establish approaches that include immediate cash savings and factors such as reputational preservation, regulatory compliance, and consumer trust. A globally agreed metric or valuation approach is needed to make investment decisions in security infrastructures somewhat subjective, which could lead to underinvestment or resource misallocation.

Interactions between value of digital security and other factors

Another open topic is the relationship between the value of digital security and external circumstances. How does the perceived value of security change in response to macroeconomic conditions, technical advancements, or shifts in society's privacy values? In an economic crisis, for example, firms may be more risk-averse, raising their perceived value of digital security to protect their limited resources. Another aspect worth investigating is the relationship between digital security and customer behaviour. Users' demand for robust security may impact product development and commercial models as they become more tech-savvy and privacy-conscious. On the other hand, a user who is unconcerned about security threats may inadvertently promote sloppy security methods. Studies into these relationships can yield significant insights, allowing organisations to foresee how external movements affect their security posture and prepare for future issues.

Observing actual behaviour versus behavioural intention

The disparity between individuals' behavioural intentions and actual behaviours is a critical gap in comprehending digital security. Whilst many people intend to follow security best practices, such as frequently updating passwords, utilising two-factor authentication, and avoiding suspicious links, the reality often paints a different image. Why is there a disconnect between what people say and what they do? Psychological, societal, and technological elements all have the potential to play a role. For example, cognitive dissonance, which occurs when people are uncomfortable because they possess contradictory ideas and behaviours, might lead to avoidance methods or excuses. Similarly, the perceived inconvenience of strict security measures may outweigh the actual threats, resulting in slack practices. Developing user-friendly security solutions that better correspond with human behaviour, education campaigns that effectively translate intentions into actions, and understanding the underlying psychological causes that underlie this disparity could all be part of research to close this gap.

Case studies

Successful digital security implementation

Case study 1: CISA and global counterparts advocate for 'Security-by-Design'

In a landmark collaboration, the Cybersecurity and Infrastructure Security Agency (CISA) (2022), along with esteemed international agencies including the FBI, NSA, and cybersecurity authorities from Australia, Canada, UK, Germany, Netherlands, and New Zealand, have released a seminal guidance titled "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default". (CISA 2023). This document underscores the pressing need for software manufacturers to embed security as an integral part of product design and configuration, aiming for a future where technology products inherently uphold security.

The advice champions several vital ideas. First, it argues for software manufacturers to take proactive responsibility for security outcomes, removing the burden from customers. This means that products will have a secure configuration as the default setting. Second, it supports radical transparency and responsibility, particularly regarding vulnerability advisories. Furthermore, a top-down strategy with executive-level pledges is advised, emphasising security as an essential component of product development.

The effort has received backing from prominent leaders from numerous worldwide cybersecurity organisations. CISA Director Jen Easterly emphasised the importance of incorporating security into product design, especially as software forms the foundation of essential systems and services. Figures from the FBI, NSA, and other agencies echoed this stance, emphasising the potential consequences of insecure technology goods for individual consumers and national security. They believe that ensuring that goods are secure by default is the first step towards a more secure digital future.

This endeavour intends to address urgent technological issues and change the manufacturing culture's thinking. It envisions a future in which cybersecurity is not an afterthought but an essential element of digital products. Such collaborative efforts are both praiseworthy and necessary as we traverse an increasingly digital landscape. The message is clear: familiarise technology manufacturers with this guidance and continue contributing to security by design and default with private sector partners. Feedback and ongoing communication are encouraged, indicating an ongoing and growing discussion about a future in which digital technology is innately secure.

The CISA guidance proposes a set of transformative principles. These are based on the idea that software manufacturers should shoulder security obligations rather than deferring them to end users. This proactive posture implies that every digital product includes the highest security specifications by default. Concurrently, the guideline extols the merits of uncompromising transparency, particularly regarding vulnerabilities, to promote a culture of trust and openness. The role of corporate leadership in promoting these concepts, emphasising security as an essential component of product development, is critical.

This collaboration of multinational cybersecurity groups, led by CISA, envisions a future in which security is not an afterthought but the foundation of every digital product. It is not just about blocking imminent dangers; it is about shaping a new industrial mindset in which security is integrally knit into the digital fabric. These coordinated global initiatives have progressed from commendable to necessary in today's computerised period. The clarion appeal has been issued for global tech manufacturers to include this direction, evolve continuously, and establish security as a cornerstone, thereby forging a future in which the digital domain is intrinsically protected.

Future of digital security

Future of digital security: navigating uncharted waters

Every step forward in the complicated interplay of technology and security presents new difficulties and opportunities. As we stand on the threshold of a new era defined by quantum computing, artificial intelligence, and ever-changing cyber threats, we urgently need to forecast what the future holds for digital security. This section provides a view of that horizon by describing prospective challenges, technical evolutions, and the legal landscape.

Predicted threats and challenges

Cyber threats are constantly changing, with attackers growing more sophisticated and ambitious. Several advancements in this area are possible:

Quantum Challenges: As quantum computing advances, traditional encryption approaches may become susceptible since quantum computers may theoretically decipher present encryption algorithms quicker than classical machines.

AI-powered Cyberattacks: Weaponising artificial intelligence may result in self-evolving malware that can adapt and respond to protective measures in real time.

Deepfakes and Misinformation: When enhanced by AI, deepfakes could create hyper-realistic but wholly fake content, potentially leading to misinformation campaigns, identity theft, or even political destabilisation.

IoT Vulnerabilities: As more devices become interconnected, cyber attackers' attack surface grows, making Internet of Things (IoT) devices potential weak links in security chains.

Anticipated technological advancements

Despite the frequent and more intense threats, the cyber security potential is enormous, with inventions ready to strengthen our digital defences:

Quantum Cryptography (Bennett and Brassard 1984, 2014, 2020; Broadbent and Schaffner 2015; Kumar 2022; NIST 2022, 2023a, 2023b; Routray et al. 2017; Shapna Akter n.d.): In parallel with the challenges offered by quantum computing, research into quantum cryptography is occurring. For example, Quantum Key Distribution (QKD) guarantees ultra-secure communication by detecting eavesdropping efforts.

Artificial Intelligence and Machine Learning in Defence (Anthi et al. 2020; Costa et al. 2023; Dar et al. 2019; Elgammal et al. 2017; Goyal et al. 2023; Karras et al. 2019; Khamaiseh et al. 2022; Liang et al. 2022; Macas et al. 2024; Ozdag 2018; Qiu et al. 2019; Rosenberg et al. 2021; Suhag and Daniel 2023; Sun et al. 2018; Thuraisingham 2020; Wallace et al. 2019; Wang et al. 2019, 2023; Zbrzezny and Grzybowski 2023; Zhang et al. 2022; Zhou et al. 2022): AI will play a critical role in defence, just as it may be weaponised for assaults. Machine learning algorithms can be trained to detect anomalies, forecast potential attack vectors, and respond to attacks in real time.

Homomorphic Encryption (Gentry 2009): This type of encryption allows data to be processed without decryption, providing additional security during data calculation processes.

Blockchain and Security (Deshmukh et al. 2022; He et al. 2022): Blockchain's decentralised and tamper-evident nature can be used for authentication processes, secure transactions, and even to protect data integrity.

Evolving legal framework

As the digital security landscape evolves, we can expect significant changes in its legal and regulatory frameworks. Cyber threats and attacks are global issues that require international collaboration to address effectively. Therefore, we can anticipate the development of more international treaties and agreements to address cybercrime, particularly those that focus on sharing cyber threat intelligence and establishing security standards.

Moreover, as data become increasingly valuable, we expect abundant legislation to protect it and promote ethical data practices. Given the potential for these technologies to impact individuals' privacy and autonomy, we can also expect to see a particular emphasis on regulating AI and big data analytics. With these strict data regulations in place, we can help ensure that digital security benefits society.

New technologies such as quantum computing and advanced artificial intelligence have the potential to revolutionise the digital security landscape. However, they also pose significant challenges, particularly in ensuring that these technologies are not weapons of mass surveillance or harm. As such, we can expect to see new regulatory approaches that balance the need for innovation with oversight and control. By regulating emerging technologies, we can limit their potential hazards whilst exploiting their potential for developing technology that benefits society.

Recommendations

Recommendations: fortifying the digital frontier

Stakeholders from all walks of life are finding themselves at the intersection of threat and innovation in the quickly evolving world of digital security. Whilst each industry presents unique problems, several universal rules may pave the path to a more secure digital future. This chapter converts ideas from prior conversations into actionable recommendations for various parties.

For individuals

Digital security is not just for technocrats and cybersecurity professionals; every internet user has a role to play. Here are some essential insights for those navigating the digital world:

- Stay Informed: Because threats are constantly evolving, from sophisticated AI-driven hacks to deepfakes, individuals must stay current on the latest dangers and defensive measures.
- Begin with Security Hygiene: Just as one communicates a solid goal for maintaining health hygiene, so should one convey a solid aim to maintain

digital hygiene. This includes updating passwords, employing multi-factor authentication, and being wary of questionable connections.

- Adopt Advanced Security Measures: As the threat landscape expands, so do the methods for combating it. Consider advanced security solutions such as homomorphic encryption and blockchain-based authentication, particularly for individuals who handle sensitive data.
- Promote and Demand Transparency: In industries such as retail and banking, consumers should demand transparency about how their data are protected. This not only keeps organisations accountable but also promotes a security culture.

For organisations

Organisations, whether healthcare facilities or manufacturing units, constitute the foundation of our digital infrastructure. They have the most to lose as well as the most to gain. Here are some suggestions for them:

- Use Industry-Specific Strategies: Because digital security varies by industry—from EHRs in healthcare to smart factories in manufacturing—it is necessary to implement industry-specific methods.
- Invest in R&D: Exploring predicted technological advances such as quantum cryptography and AI-driven defence measures can be game changers. Companies should consider spending resources on research and staying ahead of the curve.
- Bridging Intention and Action: Businesses should be aware of the gap between security intentions and actual behaviour at the employee and consumer levels. Initiatives can be launched to ensure that best practices are understood and regularly applied.
- Quantify and Communicate Value: Since identifying the tangible value of digital security is complex, organisations should build comprehensive measurements encompassing the whole range of advantages, from financial savings to reputational protection. Transparently communicating this value can help with stakeholder buy-in and security investment prioritisation.

For policymakers

The legal and regulatory landscape designers hold a great deal of responsibility. Here are some policy implications as digital dynamics unfold:

- Promote International Collaboration: Recognising that cyber risks know no boundaries, officials should advocate for international conventions and accords. This lays the groundwork for common security standards and encourages the exchange of cyber threat intelligence.
- Evolve with the Times: As emerging technologies such as quantum computing and artificial intelligence transform the digital landscape, regulatory frameworks must adapt to ensure that breakthroughs are used responsibly.

- Prioritise Education and Awareness: Policymakers can influence public education and laws. Campaigns highlighting the importance of digital security at all levels, from the individual to the institutional, can have a significant effect.
- Ensure Holistic Regulation: Future rules should address reactive and proactive measures, such as enforcing routine security assessments or encouraging innovation in digital defence mechanisms.

To summarise the findings from this chapter, digital security is seen as a collaborative effort that necessitates collaboration among individuals, organisations, and policymakers. By following this advice, each stakeholder may bolster their digital fortifications, ensuring that security remains at the forefront of the digital era.

What does this mean for crime and crime prevention in the real world?

The real-world implications of digital security on crime and crime prevention are multifaceted and critical. The evolution of digital security, highlighted through advanced technologies like AI, quantum computing, and blockchain, directly impacts the landscape of cybercrime and the strategies employed for its prevention.

The increasing sophistication of digital security measures deters common cybercrimes, including identity theft, phishing, and data breaches. However, this escalation in security prompts a corresponding advancement in criminal tactics, leading to more complex and nuanced cyber threats. These developments necessitate robust technological defences and a profound understanding of the legal and regulatory frameworks governing digital security.

Whilst designed to protect individual data rights, privacy laws also present a dual challenge. They must balance the enhancement of privacy for legitimate users and the prevention of their exploitation by criminals. This paradox necessitates sophisticated approaches to identity verification and data tracking that respect privacy yet can detect and mitigate illicit activities.

Furthermore, sector-specific digital security challenges in healthcare, finance, retail, and manufacturing industries require tailored strategies considering each sector's unique vulnerabilities. For instance, securing patient data in healthcare is vital for privacy and preventing data breaches that could lead to medical identity theft or system tampering. In finance, robust encryption and fraud detection systems are essential to protect against financial fraud.

The study underscores the importance of a holistic approach to digital security, integrating technological advancements, legal frameworks, sector-specific needs, and the psychological aspects of security practices. This comprehensive approach will enable effective crime prevention in the digital world, ensuring the security and trustworthiness of our increasingly interconnected digital society.

Conclusion: towards a resilient digital future

In this comprehensive review, we have reflected upon the significant contributions to knowledge this study has offered in the ever-evolving field of digital security. This work has synthesised existing paradigms and practices and illuminated novel intersections between technology, policy, and regulatory frameworks, offering a multifaceted perspective on digital security strategies. The analysis has encapsulated the breadth of technologies, from foundational encryption to cutting-edge artificial intelligence and blockchain developments, highlighting their pivotal role in contemporary digital security measures.

This study's key finding has been identifying and articulating industry-specific digital security challenges and the necessity for customised strategies. This insight has been instrumental in advancing the understanding that a uniform approach to digital security is impractical and often counterproductive. The research has underscored the importance of sector-specific nuances, demonstrating how tailored strategies are paramount in addressing different industries' unique digital security needs.

Furthermore, this review has made a novel contribution by integrating the concept of digital security valuation into a broader socio-technical context. We have extended the discussion beyond traditional risk-based metrics to include trust, reputation, and social well-being considerations. This holistic approach to valuing digital security represents a significant shift from conventional methodologies, offering a more comprehensive framework for understanding the impact and importance of digital security in society.

The novelty of this study has also lain in its forward-looking analysis, particularly in the context of emergent technologies and the evolving threat landscape. By examining the potential implications of quantum computing and AI-driven threats alongside the burgeoning promise of quantum cryptography and AI-enabled defences, this review has provided a visionary perspective on the future challenges and opportunities in digital security.

This review study has been characterised by its comprehensive coverage, innovative insights, and forward-thinking analysis. It has consolidated existing knowledge in the field and introduced new dimensions and perspectives, enriching the academic discourse and offering valuable guidance for practitioners and policymakers in digital security. The study's contribution to knowledge has lain in its ability to navigate the complexities of digital security, offering a nuanced understanding crucial for developing effective, future-proof security strategies in our increasingly digital world.

Appendix

Glossary of key terms

- Artificial Intelligence (AI): A branch of computer science dedicated to creating systems capable of performing tasks that normally require human intelligence. In digital security, AI can predict, identify, and combat threats in real time.
- Blockchain: A decentralised, distributed ledger technology that ensures data integrity by recording transactions in 'blocks' linked in a 'chain'. It offers transparency and security, making it resistant to tampering.
- Cloud Security: Refers to the strategies, controls, and measures designed to protect data, applications, and services housed in cloud environments.
- Digital Security: Comprehensive measures and strategies designed to protect digital devices, information, and networks from threats and attacks.
- Endpoint Security: The practice of securing endpoints or entry points of end-user devices like computers and mobile devices, ensuring they do not act as pathways for threats.
- Encryption Technologies: Methods used to convert data into a code to prevent unauthorised access. Ensures data confidentiality during storage or transmission.
- Legal Framework for Digital Security: The collection of national and international laws, regulations, and policies aimed at securing the digital space from cyber threats and upholding user privacy.
- Machine Learning: A subset of AI that allows systems to learn and improve from experience without being explicitly programmed. Utilised in security to detect patterns and anomalies.
- Network Security Solutions: A set of practices intended to protect the integrity, confidentiality, and accessibility of computer networks by preventing unauthorised access, use, malfunction, modification, or denial of a computer network and network-accessible resources.
- Privacy Laws: Legal frameworks designed to protect the personal information and data of individuals from unauthorised use or breaches.
- Quantum Computing: An area of computing focussed on the principles of quantum theory. It holds the potential to vastly increase processing power but also presents challenges to traditional encryption methods.
- Quantum Cryptography: Utilises principles of quantum mechanics to encrypt data, ensuring that it cannot be intercepted without alerting the sender and receiver.
- Sectoral Digital Security: Refers to industry-specific digital security challenges, solutions, and practices. It acknowledges the unique threats and solutions pertinent to sectors like healthcare, finance, retail, and manufacturing.
- Technological Advancements: The progression of technologies which might either enhance digital security measures or present novel threats that must be countered.

- Value of Digital Security: The perceived or quantified worth associated with the measures and strategies of cybersecurity, encompassing elements like trust, reputation, and societal well-being.

Acknowledgements Eternal gratitude to the Fulbright Visiting Scholar Project.

Author contributions Dr Petar Radanliev was responsible for reviewing the researched literature and conceiving the study, was involved in protocol development, gaining ethical approval, participants recruitment and data analysis, wrote the first draft of the manuscript, reviewed and edited the manuscript, and approved the final version.

Funding This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC [under Grant Number EP/S035362/1] and ESRC [Under Grant Number ES/V003666/1].

Data availability All data and materials are included in the article.

Declarations

Competing interests Petar Radanliev reports financial support was provided by University of Oxford. The author declares no competing interests.

Ethical approval The University of Oxford ethical committee has granted ethical approval under reference R51864/002.

References

5Is. 2002 CLAIMED framework—For mobilising preventers—CRIME FRAMEWORKS. https://crimeframeworks.com/claimed-mobilisation-of-preventers/. Accessed 23 January 2024.

Abie, H., and I. Balasingham. 2012. Risk-based adaptive security for smart IoT in eHealth. *SeTTIT 2012, September 24–26, Oslo, Norway*. https://pdfs.semanticscholar.org/c39d/04c6f3b84c77ad379d0358bfbe7148ad4fd2.pdf.

Ahmad, R., and I. Alsmadi. 2021. Machine learning approaches to IoT security: A systematic literature review. *Internet of Things* 14: 100365. https://doi.org/10.1016/j.iot.2021.100365.

Akinrolabu, O., J.R.C. Nurse, A. Martin, and S. New. 2019. Cyber risk assessment in cloud provider environments: Current models and future needs. In *Computers and security*, vol. 87, 101600. Elsevier Ltd. https://doi.org/10.1016/j.cose.2019.101600.

Altman Vilandrie & Company. 2017. Are your company's IoT devices secure? *IoT Security White Paper, June 2017*, 1–11. http://www.altvil.com/wp-content/uploads/2017/09/AVCo-IoT-Security-White-Paper-June-2017-vF.pdf.

Ani, U.P.D., J.M. Watson, B. Green, B. Craggs, and J.R.C. Nurse. 2020. Design considerations for building credible security testbeds: Perspectives from industrial control system use cases. *Journal of Cyber Security Technology*. https://doi.org/10.1080/23742917.2020.1843822.

Ani, U.D., J.D.McK. Watson, J.R.C. Nurse, A. Cook, and C. Maple. 2019. A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. In *PETRAS/IET conference living in the Internet of Things: Cybersecurity of the IoT—2019*, 1–16. http://arxiv.org/abs/1904.01551.

Anthi, E., L. Williams, and P. Burnap. 2018. Pulse: An adaptive intrusion detection for the internet of things. *Living in the Internet of Things: Cybersecurity of the IoT* 35: 4. https://doi.org/10.1049/cp.2018.0035.

Anthi, E., L. Williams, M. Rhode, P. Burnap, and A. Wedgbury. 2020. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *Journal of Information Security and Applications* 58 (May 2021-102717): 1–9. https://doi.org/10.1016/j.jisa.2020.102717.

Anthi, E., L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap. 2019. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal* 6 (5): 9042–9053. https://doi.org/10.1109/JIOT.2019.2926365.

Aria, M., and C. Cuccurullo. 2017. Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics* 11 (4): 959–975. https://doi.org/10.1016/j.joi.2017.08.007.

Ayad, A., A. Zamani, A. Schmeink, and G. Dartmann. 2019. Design and implementation of a hybrid anomaly detection system for IoT. In *2019 6th international conference on Internet of Things: Systems, management and security, IOTSMS 2019*, 87–92. https://doi.org/10.1109/IOTSMS48152.2019.8939206.

Azzi, R., R.K. Chamoun, and M. Sokhn. 2019. The power of a blockchain-based supply chain. *Computers and Industrial Engineering* 135: 582–592. https://doi.org/10.1016/j.cie.2019.06.042.

Bajoudah, S., C. Dong, and P. Missier. 2019. Toward a decentralized, trust-less marketplace for brokered IoT data trading using blockchain. In *Proceedings—2019 2nd IEEE international conference on blockchain, blockchain 2019*, 339–346. https://doi.org/10.1109/Blockchain.2019.00053.

Bär, K., Z.N.L. Herbert-Hansen, and W. Khalid. 2018. Considering Industry 4.0 aspects in the supply chain for an SME. *Production Engineering* 12 (6): 747–758. https://doi.org/10.1007/s11740-018-0851-y.

Bécue, A., I. Praça, and J. Gama. 2021. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-020-09942-2.

Bennett, C.H., and G. Brassard. 1984. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international conference on computers, systems and signal processing*, 1–8. https://web.archive.org/web/20200130165639/http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf.

Bennett, C.H., and G. Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (P1): 7–11. https://doi.org/10.1016/J.TCS.2014.05.025.

Bennett, C.H., and G. Brassard. 2020. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (P1): 7–11. https://doi.org/10.1016/j.tcs.2014.05.025.

Bhingarkar, S., S.T. Revathi, C.S. Kolli, and H.K. Mewada. 2022. An effective optimization enabled deep learning based malicious behaviour detection in cloud computing. *International Journal of Intelligent Robotics and Applications*. https://doi.org/10.1007/S41315-022-00239-X/TABLES/2.

Bommasani, R., Klyman, K., Zhang, D. and Liang, P. 2023. Do foundation model providers comply with the eu ai act. Stanford Center for Research on Foundation Models, Institute for Human-Centered Artificial Intelligence.

Botta, A., W. De Donato, V. Persico, and A. Pescapé. 2016. Integration of cloud computing and Internet of Things: A survey. *Future Generation Computer Systems* 56: 684–700. https://doi.org/10.1016/j.future.2015.09.021.

Brass, I., L. Tanczer, M. Carr, M. Elsden, and J. Blackstock. 2018. Standardising a moving target: The development and evolution of IoT security standards. *Living in the Internet of Things: Cybersecurity of the IoT—2018* 24: 9. https://doi.org/10.1049/cp.2018.0024.

Broadbent, A., and C. Schaffner. 2015. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography* 78 (1): 351–382. https://doi.org/10.1007/S10623-015-0157-4.

Caiado, R.G.G., L.F. Scavarda, L.O. Gavião, P. Ivson, D.L. de Mattos Nascimento, and J.A. Garza-Reyes. 2021. A fuzzy rule-based industry 4.0 maturity model for operations and supply chain management. *International Journal of Production Economics* 231: 107883. https://doi.org/10.1016/j.ijpe.2020.107883.

Cao, L. 2021. Artificial intelligence in retail: Applications and value creation logics. *International Journal of Retail and Distribution Management* 49 (7): 958–976. https://doi.org/10.1108/IJRDM-09-2020-0350/FULL/PDF.

Cavalcante, E., J. Pereira, M.P. Alves, P. Maia, R. Moura, T. Batista, F.C. Delicato, and P.F. Pires. 2016. On the interplay of Internet of Things and Cloud Computing: A systematic mapping study. *Computer Communications* 8990: 17–33. https://doi.org/10.1016/j.comcom.2016.03.012.

CCPA. 2018. California Consumer Privacy Act (CCPA) | State of California—Department of Justice—Office of the Attorney General. https://oag.ca.gov/privacy/ccpa.

Chamola, V., V. Hassija, V. Gupta, and M. Guizani. 2020. A comprehensive review of the COVID-19 pandemic and the role of IoT, Drones, AI, Blockchain, and 5G in managing its impact. *IEEE Access* 8: 90225–90265. https://doi.org/10.1109/ACCESS.2020.2992341.

Chang, M.C., and D. Park. 2020. How can blockchain help people in the event of pandemics such as the COVID-19? *Journal of Medical Systems*. https://doi.org/10.1007/s10916-020-01577-8.

Chanson, M., A. Bogner, D. Bilgeri, E. Fleisch, and F. Wortmann. 2019. Blockchain for the IoT: Privacy-preserving protection of sensor data. *Journal of the Association for Information Systems* 20 (9): 1271–1307. https://doi.org/10.17705/1jais.00567.

Cheikhrouhou, O., I. Amdouni, K. Mershad, M. Ammi, and T.N. Gia. 2022. Blockchain for the cybersecurity of smart city applications. https://arxiv.org/abs/2206.02760v1.

CISA. 2022. *CISA stakeholder-specific vulnerability categorization guide*. Cybersecurity and Infrastructure Security Agency.

CISA. 2023. Shifting the balance of cybersecurity risk: Principles and approaches for security-by-design and -default. http://www.cisa.gov/tlp/.

Clarke, R.V. 1995. Situational crime prevention. *Crime and justice* 19: 91–150.

Cook, Gary and J. Van Horn. 2011. How dirty is your data? A look at the energy choices that power cloud computing. http://www.greenpeace.org/international/Global/international/publications/climate/2011/Cool%20IT/dirty-data-report-greenpeace.pdf.

Costa, J.C., T. Roxo, H. Proença, S. Member, and P.R.M. Inácio. 2023. How deep learning sees the world: A survey on adversarial attacks & defenses. *arXiv* 12: 61113–61136. https://doi.org/10.1109/ACCESS.2024.3395118.

Council of Europe. 2001. Budapest convention—Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Craggs, B., and A. Rashid. 2017. Smart cyber-physical systems: Beyond usable security to security ergonomics by design. In *2017 IEEE/ACM 3rd international workshop on software engineering for smart cyber-physical systems (SEsCPS)*, 22–25. https://doi.org/10.1109/SEsCPS.2017.5.

Crawford, D., and J. Sherman. 2018. Gaps in United States federal government IoT security and privacy policies. *Journal of Cyber Policy* 3 (2): 187–200. https://doi.org/10.1080/23738871.2018.1514061.

Dalenogare, L.S., G.B. Benitez, N.F. Ayala, and A.G. Frank. 2018. The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Production Economics* 204: 383–394. https://doi.org/10.1016/J.IJPE.2018.08.019.

Dar, S.U.H., M. Yurt, L. Karacan, A. Erdem, E. Erdem, and T. Cukur. 2019. Image synthesis in multi-contrast MRI with conditional generative adversarial networks. *IEEE Transactions on Medical Imaging* 38 (10): 2375–2388. https://doi.org/10.1109/TMI.2019.2901750.

de Bruin, B., and L. Floridi. 2017. The ethics of cloud computing. *Science and Engineering Ethics* 23 (1): 21–39. https://doi.org/10.1007/s11948-016-9759-0.

Deshmukh, A., N. Sreenath, A.K. Tyagi, and U.V.E. Abhichandan. 2022. Blockchain enabled cyber security: A comprehensive survey. In *2022 international conference on computer communication and informatics, ICCCI 2022*. https://doi.org/10.1109/ICCCI54379.2022.9740843.

Diamanti, E., H.K. Lo, B. Qi, and Z. Yuan. 2016. Practical challenges in quantum key distribution. *npj Quantum Information* 2 (1): 1–12. https://doi.org/10.1038/npjqi.2016.25.

Díaz, M., C. Martín, and B. Rubio. 2016. State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing. *Journal of Network and Computer Applications* 67: 99–117. https://doi.org/10.1016/j.jnca.2016.01.010.

Dong, Z., F. Luo, and G. Liang. 2018. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. *Journal of Modern Power Systems and Clean Energy* 6 (5): 958–967. https://doi.org/10.1007/S40565-018-0418-0/FIGURES/5.

Ekblom, P. 2017. Technology, opportunity, crime and crime prevention: Current and evolutionary perspectives. In *Crime prevention in the 21st century: Insightful approaches for crime prevention initiatives*, 319–343. https://doi.org/10.1007/978-3-319-27793-6_19.

Elgammal, A., B. Liu, M. Elhoseiny, and M. Mazzone. 2017. CAN: Creative adversarial networks, generating "Art" by learning about styles and deviating from style norms. In *Proceedings of the 8th* *international conference on computational creativity, ICCC 2017*. https://arxiv.org/abs/1706.07068v1.

ENISA. 2009. Cloud computing risk assessment. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment.

ENISA. 2023a. Cybersecurity of AI and Standardisation—ENISA. https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation.

ENISA. 2023b. The EU Cybersecurity Act | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

European Parliament. 2023. AI Act: A step closer to the first rules on Artificial Intelligence | News | European Parliament. https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

FACT SHEET: Biden-Harris Administration Announces New Actions to Promote Responsible AI Innovation That Protects Americans' Rights and Safety | The White House. 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-new-actions-to-promote-responsible-ai-innovation-that-protects-americans-rights-and-safety/.

Faller, C., and D. Feldmüller. 2015. Industry 4.0 learning factory for regional SMEs. *Procedia CIRP* 32: 88–91. https://doi.org/10.1016/j.procir.2015.02.117.

Faqir-Rhazoui, Y., J. Arroyo, and S. Hassan. 2021. A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain. *Journal of Internet Services and Applications* 12 (1): 1–20. https://doi.org/10.1186/S13174-021-00139-6/TABLES/5.

Fatorachian, H., and H. Kazemi. 2021. Impact of Industry 4.0 on supply chain performance. *Production Planning and Control* 32 (1): 63–81. https://doi.org/10.1080/09537287.2020.1712487.

Feng, X., M. Conrad, and K. Hussein. 2022. NHS big data intelligence on blockchain applications, 191–208. https://doi.org/10.1007/978-3-030-87954-9_8.

GDPR. 2018. What is GDPR, the EU's new data protection law?—GDPR.eu. https://gdpr.eu/what-is-gdpr/.

Gentry, C. 2009. Fully homomorphic encryption using ideal lattices. In *Proceedings of the annual ACM symposium on theory of computing*, 169–178. https://doi.org/10.1145/1536414.1536440.

Ghirardello, K., C. Maple, D. Ng, and P. Kearney. 2018. Cyber security of smart homes: Development of a reference architecture for attack surface analysis. *Living in the Internet of Things: Cybersecurity of the IoT—2018* 45: 10. https://doi.org/10.1049/cp.2018.0045.

Ghodmare, S.D., B.V. Khode, and S.M. Ladekar. 2021. The role of artificial intelligence in industry 4.0 and smart city development. In *Lecture notes in civil engineering*, vol. 87, 591–604. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-981-15-6463-5_58.

Gordon, L.A., and M.P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5 (4): 438–457. https://doi.org/10.1145/581271.581274.

Goyal, S., S. Doddapaneni, M.M. Khapra, and B. Ravindran. 2023. A survey of adversarial defenses and robustness in NLP. *ACM Computing Surveys*. https://doi.org/10.1145/3593042.

Gunasekaran, A., N. Subramanian, and W.T.E. Ngai. 2018. Quality management in the 21st century enterprises: Research pathway towards Industry 4.0. *International Journal of Production Economics*. https://doi.org/10.1016/J.IJPE.2018.09.005.

Hajizadeh, M., M. Alaeddini, and P. Reaidy. 2023. Bibliometric analysis on the convergence of artificial intelligence and blockchain. In *Lecture notes in networks and Systems*, *595 LNNS*, 334–344. https://doi.org/10.1007/978-3-031-21229-1_31/COVER.

Hamid, O.H. 2022. From model-centric to data-centric AI: A paradigm shift or rather a complementary approach? In *8th international conference on information technology trends: Industry 4.0: Technology trends and solutions, ITT 2022*, 196–199. https://doi.org/10.1109/ITT56123.2022.9863935.

Hazra, A., A. Alkhayyat, and M. Adhikari. 2022. Blockchain-aided integrated edge framework of cybersecurity for Internet of Things. *IEEE Consumer Electronics Magazine*. https://doi.org/10.1109/MCE.2022.3141068.

He, S., E. Ficke, M.M.A. Pritom, H. Chen, Q. Tang, Q. Chen, M. Pendleton, L. Njilla, and S. Xu. 2022. Blockchain-based automated and robust cyber security management. *Journal of Parallel and Distributed Computing* 163: 62–82. https://doi.org/10.1016/J.JPDC.2022.01.002.

HIPAA. 1996. Health insurance portability and accountability act of 1996 (HIPAA) | CDC. https://www.cdc.gov/phlp/publications/topic/hipaa.html.

Hofmann, E., and M. Rüsch. 2017. Industry 4.0 and the current status as well as future prospects on logistics. *Computers in Industry* 89: 23–34. https://doi.org/10.1016/j.compind.2017.04.002.

ICO. 2018. *Information Commissioner's Office (ICO): The UK GDPR*. UK GDPR Guidance and Resources. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/.

Ishmaev, G. 2019. The ethical limits of blockchain-enabled markets for private IoT data. *Philosophy and Technology*. https://doi.org/10.1007/s13347-019-00361-y.

Jalali, M.S., J.P. Kaiser, M. Siegel, and S. Madnick. 2019. The Internet of Things promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products. *IEEE Security & Privacy* 17 (2): 39–48. https://doi.org/10.1109/MSEC.2018.2888780.

Van Eck, N. and Waltman, L., 2010. Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics* 84 (2): 523–538. https://doi.org/10.1007/s11192-009-0146-3.

Javaid, A., M. Zahid, I. Ali, R.J.U.H. Khan, Z. Noshad, and N. Javaid. 2020. Reputation system for IoT data monetization using blockchain. In *Lecture notes in networks and systems*, vol. 97, 173–184. Springer. https://doi.org/10.1007/978-3-030-33506-9_16.

Jazdi, N. 2014. Cyber physical systems in the context of Industry 4.0. In *2014 IEEE international conference on automation, quality and testing, robotics*, 1–4. https://doi.org/10.1109/AQTR.2014.6857843.

Karras, T., S. Laine, and T. Aila. 2019. A style-based generator architecture for generative adversarial networks. In *Proceedings of the IEEE computer society conference on computer vision and pattern recognition*, *2019-June*, 4396–4405. https://doi.org/10.1109/CVPR.2019.00453.

Khamaiseh, S.Y., D. Bagagem, A. Al-Alaj, M. Mancino, and H.W. Alomari. 2022. Adversarial deep learning: A survey on adversarial attacks and defense mechanisms on image classification. *IEEE Access* 10: 102266–102291. https://doi.org/10.1109/ACCESS.2022.3208131.

Kolberg, D., and D. Zühlke. 2015. Lean automation enabled by industry 4.0 technologies. *IFAC-PapersOnLine* 48 (3): 1870–1875. https://doi.org/10.1016/j.ifacol.2015.06.359.

Kumar, M. 2022. Post-quantum cryptography algorithm's standardization and performance analysis. *Array* 15: 100242. https://doi.org/10.1016/J.ARRAY.2022.100242.

Kumar, M., N. Nikhil, and R. Singh. 2020. Decentralising finance using decentralised blockchain oracles. In *2020 international conference for emerging technology, INCET 2020*. https://doi.org/10.1109/INCET49848.2020.9154123.

Latvala, S., M. Sethi, and T. Aura. 2020. Evaluation of out-of-band channels for IoT security. *SN Computer Science* 1 (1): 1–17. https://doi.org/10.1007/s42979-019-0018-8.

Lawrenz, S., P. Sharma, and A. Rausch. 2019. Blockchain technology as an approach for data marketplaces. *ACM International Conference Proceeding Series, Part F* 1481: 55–59. https://doi.org/10.1145/3320154.3320165.

Lee, J., B. Bagheri, and H.-A. Kao. 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters* 3: 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001.

Lee, J., H.-A. Kao, and S. Yang. 2014. Service innovation and smart analytics for industry 4.0 and big data environment. *Procedia CIRP* 16: 3–8. https://doi.org/10.1016/j.procir.2014.02.001.

Lezzi, M., M. Lazoi, and A. Corallo. 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry* 103: 97–110. https://doi.org/10.1016/j.compind.2018.09.004.

Liang, H., E. He, Y. Zhao, Z. Jia, and H. Li. 2022. Adversarial attack and defense: A survey. *Electronics* 11 (8): 1283. https://doi.org/10.3390/ELECTRONICS11081283.

Liao, Y., F. Deschamps, E. de Freitas Rocha Loures, and L.F.P. Ramos. 2017. Past, present and future of Industry 4.0—A systematic literature review and research agenda proposal. *International Journal of Production Research* 55 (12): 3609–3629. https://doi.org/10.1080/00207543.2017.1308576.

Liu, M., W. Yeoh, F. Jiang, and K.K.R. Choo. 2021. Blockchain for cybersecurity: Systematic literature review and classification. *Journal of Computer Information Systems* 62 (6): 1182–1198. https://doi.org/10.1080/08874417.2021.1995914.

Lucio, Y.I.L., K. Marceles Villalba, and S.A. Donado. 2022. Adaptive blockchain technology for a cybersecurity framework in IIoT. *Revista Iberoamericana de Tecnologias Del Aprendizaje* 17 (2): 178–184. https://doi.org/10.1109/RITA.2022.3166857.

Macas, M., C. Wu, and W. Fuertes. 2024. Adversarial examples: A survey of attacks and defenses in deep learning-enabled cybersecurity systems. *Expert Systems with Applications* 238: 122223. https://doi.org/10.1016/J.ESWA.2023.122223.

Mahmood, S., M. Chadhar, and S. Firmin. 2022. Cybersecurity challenges in blockchain technology: A scoping review. *Human Behavior and Emerging Technologies* 2022: 1–11. https://doi.org/10.1155/2022/7384000.

Ministry of Economy Industry and Competitiveness Accessibility. 2015. *Industria Conectada 4.0: La transformación digital de la industria española Dossier de prensa*. Ministry of Economy Industry and Competitiveness Accessibility. http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/Documents/081015%20Dossier%20prensa%20Industria%204.0.pdf.

Miotto, R., L. Li, B.A. Kidd, and J.T. Dudley. 2016. Deep patient: An unsupervised representation to predict the future of patients from the electronic health records. *Scientific Reports* 6 (1): 1–10. https://doi.org/10.1038/srep26094.

Mishra, S. 2023. Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences* 13 (10): 5875. https://doi.org/10.3390/APP13105875.

Mogavero, F., I. Visconti, A. Vitaletti, and M. Zecchini. 2021. The blockchain quadrilemma: When also computational effectiveness matters. In *Proceedings—IEEE symposium on computers and communications*, *2021-September*. https://doi.org/10.1109/ISCC53001.2021.9631511.

Mozumder, M.A.I., M.M. Sheeraz, A. Athar, S. Aich, and H.-C. Kim. 2022. Overview: Technology roadmap of the future trend of metaverse based on IoT, Blockchain, AI technique, and medical domain metaverse activity. In *International conference on advanced communication technology (ICACT)*, 256–261. https://doi.org/10.23919/ICACT53585.2022.9728808.

Müller, J.M., O. Buliga, and K.-I. Voigt. 2018. Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. *Technological Forecasting and Social Change*. https://doi.org/10.1016/J.TECHFORE.2017.12.019.

Nawir, M., A. Amir, N. Yaakob, and O.B. Lynn. 2016. Internet of Things (IoT): Taxonomy of security attacks. In *2016 3rd international conference on electronic design (ICED)*, 321–326. https://doi.org/10.1109/ICED.2016.7804660.

Nguyen, D.D., and M.I. Ali. 2019. Enabling on-demand decentralized IoT collectability marketplace using blockchain and crowdsensing. In *Global IoT summit, GIoTS 2019—Proceedings*. https://doi.org/10.1109/GIOTS.2019.8766346.

NIST. 2001. Advanced encryption standard (AES). https://web.archive.org/web/20170312045558/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

NIST. 2022. Post-quantum cryptography PQC. https://csrc.nist.gov/Projects/post-quantum-cryptography.

NIST. 2023a. Post-quantum cryptography | CSRC | competition for post-quantum cryptography standardisation. In *NISTIR 8413*. https://csrc.nist.gov/projects/post-quantum-cryptography.

NIST. 2023b. Post-quantum cryptography | CSRC | selected algorithms: Public-key encryption and key-establishment algorithms. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

Ozdag, M. 2018. Adversarial attacks and defenses against deep neural networks: A survey. *Procedia Computer Science* 140: 152–161. https://doi.org/10.1016/J.PROCS.2018.10.315.

Pan, M., J. Sikorski, C.A. Kastner, J. Akroyd, S. Mosbach, R. Lau, and M. Kraft. 2015. Applying Industry 4.0 to the Jurong Island eco-industrial park. *Energy Procedia* 75: 1536–1541. https://doi.org/10.1016/j.egypro.2015.07.313.

Payton, T. 2018. Staying safe in an increasingly interconnected world: IOT and Cybersecurity. *Cyber Security* 2 (1): 66–72.

Peasley, S., R. Waslo, T. Lewis, R. Hajj, and R. Carton. 2017. Industry 4.0 and cybersecurity Managing risk in an age of connected production. https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf.

Peukert, S., S. Treber, S. Balz, B. Haefner, and G. Lanza. 2020. Process model for the successful implementation and demonstration of SME-based industry 4.0 showcases in global production networks. *Production Engineering*. https://doi.org/10.1007/s11740-020-00953-0.

Porambage, P., T. Kumar, M. Liyanage, J. Partala, L. Lovén, M. Ylianttila, and T. Seppänen. 2019. Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI BrainICU-Measuring brain function during intensive care View project ECG-based emotion recognition View project Sec-EdgeAI: AI for Edge Security Vs Security for Edge AI. https://www.researchgate.net/publication/330838792.

Prakash, R., V.S. Anoop, and S. Asharaf. 2022. Blockchain technology for cybersecurity: A text mining literature analysis. *International Journal of Information Management Data Insights* 2 (2): 100112. https://doi.org/10.1016/J.JJIMEI.2022.100112.

Qiu, S., Q. Liu, S. Zhou, and C. Wu. 2019. Review of artificial intelligence adversarial attack and defense technologies. *Applied Sciences* 9 (5): 909. https://doi.org/10.3390/APP9050909.

Radanliev, P. 2019. Digital supply chains for industry 4.0 taxonomy of approaches. *University of Oxford Combined Working Papers and p, April*. https://doi.org/10.20944/preprints201904.0160.v1.

Radanliev, P., D. De Roure, R. Nicolescu, M. Huth, and O. Santos. 2021. Artificial intelligence and the Internet of Things in Industry 4.0. *CCF Transactions on Pervasive Computing and Interaction*. https://doi.org/10.1007/s42486-021-00057-3.

Radanliev, P., D. De Roure, J.R.C. Nurse, R. Nicolescu, M. Huth, S. Cannady, and R. Mantilla Montalvo. 2018. Integration of cyber security frameworks, models and approaches for building design principles for the Internet-of-Things in Industry 4.0. *Institution of Engineering and Technology, Living in the Internet of Things: Cybersecurity of the IoT* 41: 6. https://doi.org/10.1049/cp.2018.0041.

Rajakumaran, G., N. Venkataraman, and R.R. Mukkamala. 2020. Denial of service attack prediction using gradient descent algorithm. *SN Computer Science* 1 (1): 1–8. https://doi.org/10.1007/s42979-019-0043-7.

Sampson, R., John E.. Eck, and Jessica Dunham. 2010. Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure | Office of Justice Programs. *Security Journal* 23: 37–51.

Ranganthan, V.P., R. Dantu, A. Paul, P. Mears, and K. Morozov. 2018. A decentralized marketplace application on the Ethereum blockchain. In *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*, 90–97. https://doi.org/10.1109/CIC.2018.00023.

Reischauer, G. 2018. Industry 4.0 as policy-driven discourse to institutionalize innovation systems in manufacturing. *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2018.02.012.

Rinaldi, S., P. Bellagente, P. Ferrari, A. Flammini, and E. Sisinni. 2019. Are cloud services aware of time? An experimental analysis oriented to industry 4.0. In *IEEE international symposium on precision clock synchronization for measurement, control, and communication, ISPCS*, *2019-September*. https://doi.org/10.1109/ISPCS.2019.8886642.

Rivas, A., L. Martín, I. Sittón, P. Chamoso, J.J. Martín-Limorti, J. Prieto, and A. González-Briones. 2018. Semantic analysis system for industry 4.0. *Communications in Computer and Information Science* 877: 537–548. https://doi.org/10.1007/978-3-319-95204-8_45.

Rivest, R.L., A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21 (2): 120–126. https://doi.org/10.1145/359340.359342.

Rogers, R.W. 1975. A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology* 91 (1): 93–114. https://doi.org/10.1080/00223980.1975.9915803.

Roopak, M., G. Yun Tian, and J. Chambers. 2019. Deep learning models for cyber security in IoT networks. In *2019 IEEE 9th annual computing and communication workshop and conference, CCWC 2019*, 452–457. https://doi.org/10.1109/CCWC.2019.8666588.

Rosenberg, I., Shabtai, A., Elovici, Y. and Rokach, L., 2021. Adversarial machine learning attacks and defense methods in the cyber security domain. *ACM Computing Surveys (CSUR)* 54 (5): 1–36. https://doi.org/10.1145/3453158.

Roumani, M.A., C.C. Fung, S. Rai, and H. Xie. 2016. Value analysis of cyber security based on attack types. *ITMSOC Transactions on Innovation & Business Engineering* 01: 34–39.

Routray, S.K., M.K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar. 2017. Quantum cryptography for IoT: A perspective. In *IEEE international conference on IoT and its applications, ICIOT 2017*. https://doi.org/10.1109/ICIOTA.2017.8073638.

Russell, B., and D. Van Duren. 2016. Practical internet of things security: A practical, indispensable security guide that will navigate you through the complex realm of securely building and deploying systems in our IoT-connected world. https://www.packtpub.com/hardware-and-creative/practical-internet-things-security.

Ryan, R.M., and E.L. Deci. 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist* 55 (1): 68–78. https://doi.org/10.1037/0003-066X.55.1.68.

Ryan, R.M., and E.L. Deci. 2017. *Self-determination theory: Basic psychological needs in motivation, development, and wellness*. https://doi.org/10.1521/978.14625/28806.

Sachdev, D. 2019. Enabling data democracy in supply chain using blockchain and IoT. *Journal of Management (JOM)* 6 (1): 66–83.

Schlatt, V., T. Guggenberger, J. Schmid, and N. Urbach. 2023. Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity. *International Journal of Information Management* 68: 102470. https://doi.org/10.1016/J.IJINFOMGT.2022.102470.

Schlechtendahl, J., M. Keinert, F. Kretschmer, A. Lechler, and A. Verl. 2014. Making existing production systems Industry 4.0-ready: Holistic approach to the integration of existing production systems in Industry 4.0 environments. *Production Engineering* 9 (1): 143–148. https://doi.org/10.1007/s11740-014-0586-3.

Sehgal, N.K., P.C.P. Bhatt, J.M. Acken, N.K. Sehgal, P.C.P. Bhatt, and J.M. Acken. 2020. Cloud computing pyramid. *Cloud Computing with Security*. https://doi.org/10.1007/978-3-030-24612-9_3.

Shao, X.F., W. Liu, Y. Li, H.R. Chaudhry, and X.G. Yue. 2021. Multistage implementation framework for smart supply chain management under industry 4.0. *Technological Forecasting and Social Change* 162: 120354. https://doi.org/10.1016/j.techfore.2020.120354.

Akter, M.S., Rodriguez-Cardenas, J., Shahriar, H., Cuzzocrea, A. and Wu, F., 2023, December. Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions. In 2023 IEEE International Conference on Big Data (BigData) (pp. 5408–5417). IEEE.

Sittón-Candanedo, I. 2020. A new approach: Edge computing and blockchain for industry 4.0. *Advances in Intelligent Systems and Computing* 1004: 201–204. https://doi.org/10.1007/978-3-030-23946-6_25.

Sokolov, B., and D. Ivanov. 2015. Integrated scheduling of material flows and information services in industry 4.0 supply networks. *IFAC-PapersOnLine* 48 (3): 1533–1538. https://doi.org/10.1016/j.ifacol.2015.06.304.

Sparks, E.R., A. Talwalkar, D. Haas, M.J. Franklin, M.I. Jordan, and T. Kraska. 2015. Automating model search for large scale machine learning. *ACM SoCC 2015—Proceedings of the 6th ACM symposium on cloud computing*, 368–380. https://doi.org/10.1145/2806777.2806945.

Stock, T., and G. Seliger. 2016. Opportunities of sustainable manufacturing in industry 4.0. *Procedia CIRP* 40: 536–541. https://doi.org/10.1016/j.procir.2016.01.129.

Suhag, A., and D.A. Daniel. 2023. Study of statistical techniques and artificial intelligence methods in distributed denial of service (DDOS) assault and defense. *Journal of Cyber Security Technology* 7 (1): 21–51. https://doi.org/10.1080/23742917.2022.2135856.

Sultana, N., N. Chilamkurti, W. Peng, and R. Alhadad. 2019. Survey on SDN based network intrusion detection system using machine learning approaches. *Peer-to-Peer Networking and Applications* 12 (2): 493–501. https://doi.org/10.1007/s12083-017-0630-0.

Sun, L., M. Tan, and Z. Zhou. 2018. A survey of practical adversarial example attacks. *Cybersecurity* 1 (1): 1–9. https://doi.org/10.1186/S42400-018-0012-9/FIGURES/7.

Sung, T.K. 2017. Industry 4.0: A Korea perspective. *Technological Forecasting and Social Change*. https://doi.org/10.1016/J.TECHFORE.2017.11.005.

Sunyaev, A. 2020. Cloud computing. In *Internet computing*, 195–236. Springer International Publishing. https://doi.org/10.1007/978-3-030-34957-8_7.

Tanczer, L.M., I. Steenmans, M. Elsden, J. Blackstock, and M. Carr. 2018. Emerging risks in the IoT ecosystem: Who's afraid of the big bad smart fridge? *Living in the Internet of Things: Cybersecurity of the IoT*. https://doi.org/10.1049/cp.2018.0033.

Thuraisingham, B. 2020. The role of artificial intelligence and cyber security for social media. In *Proceedings—2020 IEEE 34th international parallel and distributed processing symposium workshops, IPDPSW 2020*, 1116–1118. https://doi.org/10.1109/IPDPSW50202.2020.00184.

Vinayakumar, R., M. Alazab, K.P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman. 2019. Deep learning approach for intelligent intrusion detection system. *IEEE Access* 7: 41525–41550. https://doi.org/10.1109/ACCESS.2019.2895334.

Wallace, E., S. Feng, N. Kandpal, M. Gardner, and S. Singh. 2019. *Universal adversarial triggers for attacking and analyzing NLP*, 2153–2162. https://doi.org/10.18653/V1/D19-1221.

Wan, J., D. Zhang, Y. Sun, K. Lin, C. Zou, and H. Cai. 2014. VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. *Mobile Networks and Applications* 19 (2): 153–160. https://doi.org/10.1007/s11036-014-0499-6.

Wang, W., F. Di Maio, and E. Zio. 2019. Adversarial risk analysis to allocate optimal defense resources for protecting cyber-physical systems from cyber attacks. *Risk Analysis* 39 (12): 2766–2785. https://doi.org/10.1111/risa.13382.

Wang, Y., T. Sun, S. Li, X. Yuan, W. Ni, E. Hossain, and H.V. Poor. 2023. Adversarial attacks and defenses in machine learning-empowered communication systems and networks: A contemporary survey. *IEEE Communications Surveys and Tutorials* 25 (4): 2245–2298. https://doi.org/10.1109/COMST.2023.3319492.

Waslo, R., T. Lewis, R. Hajj, and R. Carton. 2017. *Industry 4.0 and cybersecurity in the age of connected production | Deloitte University Press*. Deloitte University Press. https://dupress.deloitte.com/dup-us-en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html.

Weyer, S., M. Schmitt, M. Ohmer, and D. Gorecky. 2015. Towards Industry 4.0—Standardization as the crucial challenge for highly modular, multi-vendor production systems. *IFAC-PapersOnLine* 48 (3): 579–584. https://doi.org/10.1016/j.ifacol.2015.06.143.

Wortley, R., A. Sidebottom, N. Tilley, and G. Laycock. 2018. What is crime science? *Routledge Handbook of Crime Science*. https://doi.org/10.4324/9780203431405-1.

Wylde, V., N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, and J. Platts. 2022. Cybersecurity, data privacy and blockchain: A review. *SN Computer Science* 3 (2): 1–12. https://doi.org/10.1007/S42979-022-01020-4.

Xu, M., X. Chen, and G. Kou. 2019a. A systematic review of blockchain. *Financial Innovation* 5 (1): 1–14. https://doi.org/10.1186/S40854-019-0147-Z/FIGURES/2.

Xu, W., D. Hu, K.R. Lang, and J.L. Zhao. 2022. Blockchain and digital finance. *Financial Innovation* 8 (1): 1–4. https://doi.org/10.1186/S40854-022-00420-Y/METRICS.

Xu, X., Q. Liu, Y. Luo, K. Peng, X. Zhang, S. Meng, and L. Qi. 2019b. A computation offloading method over big data for IoT-enabled cloud-edge computing. *Future Generation Computer Systems* 95: 522–533. https://doi.org/10.1016/j.future.2018.12.055.

Yin, H., M. Xue, Y. Xiao, K. Xia, and G. Yu. 2019. Intrusion detection classification model on an improved k-dependence Bayesian network. *IEEE Access* 7: 157555–157563. https://doi.org/10.1109/ACCESS.2019.2949890.

Zbrzezny, A.M., and A.E. Grzybowski. 2023. Deceptive tricks in artificial intelligence: Adversarial attacks in ophthalmology. *Journal of Clinical Medicine*. https://doi.org/10.3390/JCM12093266.

Zhang, Q., S. Jia, B. Chang, and B. Chen. 2018. Ensuring data confidentiality via plausibly deniable encryption and secure deletion—A survey. *Cybersecurity* 1 (1): 1–20. https://doi.org/10.1186/s42400-018-0005-8.

Zhang, Z., H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.K.R. Choo. 2022. Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review* 55 (2): 1029–1053. https://doi.org/10.1007/S10462-021-09976-0/TABLES/6.

Zhou, S., C. Liu, D. Ye, T. Zhu, W. Zhou, and P.S. Yu. 2022. Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity. *ACM Computing Surveys*. https://doi.org/10.1145/3547330.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Terms and Conditions