BRL Working Paper Series No. 17

A bibliometric review of research on digital identity

Lennart Ante [1, 2, *], Constantin Fischer [1], Elias Strehle [1]

[1] Blockchain Research Lab, Max-Brauer-Allee 46, 22765 Hamburg
[2] Universität Hamburg, Von-Melle-Park 5, 20146 Hamburg

[*] ante@blockchainresearchlab.org

Published: 09 Feb 2021

Abstract: In recent years, potentially disruptive identity-related topics emerged, such as digital twin technology for product lifecycle management or self-sovereign identity (SSI) for sovereign data control. In this study, we identify research streams and emerging trends in academic research on digital identity through a bibliometric analysis of 1,395 peer-reviewed articles and their 44,412 references. We derive seven distinct research streams and their interrelations by means of co-citation analysis. We name the seven research streams: i) Digital twin technology for smart manufacturing and industrial health monitoring, ii) identity-based signcryption schemes, iii) distributed networks and user privacy, iv) user authentication in wireless sensor networks, v) attribute-based encryption schemes, vi) secure data exchange in the Internet of Things and vii) blockchain and smart contracts for secure data management. Each stream's high-impact publications and its development over time are reviewed and the interrelation between publications and streams are visualized. In addition, we extract directions for future research from the field's most influential publications. The results offer a comprehensive and systematic overview of publications and discourses in digital identity research.

Keywords: Digital Twin; Internet of Things; Industry 4.0; Blockchain; Smart Manufacturing; Identity Management

1 Introduction

Digital identity has high relevance for individuals, organizations, governments and objects, as identification represents a necessary basis for transactions. In the past, contracts, trade and agreements were almost exclusively handled in person (face-to-face). Today, a large proportion of transactions is handled digitally. Depending on the case, this requires a form of digital identification or authentication, i.e. the digital identity, which enables counterparties to clearly

The authors received funding through the project STEREO, which has been funded through the framework of the showcase programme Secure Digital Identities of the Bundesministerium für Wirtschaft und Energie (BMWi) under funding code 01MN200006E. The funding source was not involved in the study apart from the financial support.

identify persons, devices or objects in the virtual world. Since transactions on the Internet of Things increasingly take place directly between objects and devices (Atzori et al., 2010; S. Li et al., 2018; Sisinni et al., 2018; Wollschlaeger et al., 2017), secure methods of digital identification become even more important.

In his influential blog post "The Laws of Identity", Cameron (2005) defines a digital identity as "a set of claims made by one digital subject about itself or another digital subject." He points out that the internet lacks the "essential capability" of an identity layer, which has resulted in numerous workarounds. Allen (2016) distinguishes four evolutionary steps of online identity or identity management:

1. *Centralized identities*, where control is administered by a central authority. Examples are organizations like IANA (IP addresses), ICANN (domain names) or certificate authorities (CAs). Centralized identities come with issues like dependencies, lock-in effects and single points of failure.
2. *Federated identities*, where users can use the same identity for multiple sites and applications. The same information is stored across multiple identity management systems and users can use single sign-on (SSO) across multiple systems or organizations. Common examples for federated identities are the login facilities of Google, Facebook, Twitter and LinkedIn.
3. *User-centric identities*, where identities are administered individually or across multiple authorities without the need for federation. Users must consent to the disclosure or modification of their data. In the Internet of Things, this form of online identification management is broadened to also include "thing-centric identities" (Pal et al., 2019).
4. *Self-sovereign identities (SSI)*, where users have full autonomy over their identities. They decide if, when and how they want to disclose or modify their data. As a secure SSI requires a decentralized infrastructure, blockchain technology can provide an essential basis for SSI implementation (Ferdous et al., 2019; van Bokkem et al., 2019).

Research on digital identity has become increasingly popular in recent years. Advances in technology and an increasing desire to keep the power of centralized identity providers in check have sparked discussion and innovation among academics and practitioners. To our knowledge, no systematic bibliometric study of digital identity research exists. Studies have reviewed identities in general (Blue et al., 2018), non-technical assumptions in digital identity architectures (Bazarhanova and Smolander, 2020), blockchain-based identity management systems (Liu et al., 2020) and SSI in the healthcare sector (Houtan et al., 2020). But no study so far has systematically and comprehensively analysed the existing research on digital. Accordingly, we aim to work on this very. New and emerging technological developments such as SSI, blockchain, Internet of Things, digital twin or smart contracts are explicitly part of the examination.

Our overview of the current research environment intends to offer a starting point for researchers entering the field of digital identity and a comprehensive reference for already active researchers. As part of our work, we systematically extract 1395 articles on the topic of digital identity. This data are descriptively analyzed to identify metrics such as the number of publications over time, the most relevant publishing sources and most-cited articles. In addition, the most frequently used keywords are clustered based on their co-occurrence. Next,

we identify the intellectual discourses in the field based on co-citations and review the most relevant publications of each discourse. In addition, we determine how these discourses are related. This is particularly relevant as digital identity as a concept is still evolving and has proven to be highly interdisciplinary, connecting technology, economics and the law. Finally, we present a systematic overview of future research topics which are described in high-impact publications.

The results allow for a better and up-to-date understanding of the ever-changing construct of digital identity. They provide a basis for familiarizing oneself more easily with the subject, understanding trends, streams and interrelationships, and being able to place one's own (future) scientific projects in the overall scope of digital identity research.

The remainder of the paper is structured as follows. Section 2 describes methods and data. Section 3 presents the scope of digital identity research. First, Section 3.1 provides an overview of current publishing trends, followed by an overview of identified research streams in Section 3.2. Each research stream is summarized and reviewed in a subsection before the interrelations of research streams are shown in Section 3.3. Section 4 concludes by discussing and summarizing the results and outlining implications.

2 Methods and data

2.1 Search terms and literature data

Our study follows a bibliometric, empirical approach. We collect data from the Web of Science database in April 2020 using the search terms and methodology shown in Table 1. We use two sets of search terms to assess titles and abstracts of articles. The first comprises general terms and concepts such as “digital identity” and “user identity.” The second combines “identity” with emerging technologies such as “Internet of Things” and “blockchain.” In line with bibliometric practice (Zupic and Čater, 2015), only peer-reviewed articles, chapters and conference proceedings (Web of Science filter “Article”) are considered, which ensures a certain degree of quality. We search across all available indexes (cf. Table 1) and merge the results from both resulting literature data sets to arrive at a combined data set of 1,452 publications after filtering out duplicate entries. We remove 57 of these articles that do not fit thematically to the investigation as the result of a manual screening of titles and abstracts[1], which results in a primary set of 1,395 publications. This primary set is analysed in Section 3.1.

From the primary set of 1,395 publications, we extract all references, arriving at 44,412 publications. We follow standard practice by limiting our analysis to the most important citing publications, as they represent the greatest contribution to the research discourse (Chen and Leimkuhler, 1986). Considering only publications which were cited at least five times in our primary set of 1,395 articles, we arrive at our secondary set of 480 publications. They represent about one percent of all references, but arguably by far the most relevant publications.

[1] The majority of these 57 articles deal with digital identity in the context of evolutionary biology.

Table 1. Search terms and results.

Procedure	No. of Articles
Search terms 1: *TS=("digital identit*" OR "online identit*" OR "user identit*" OR "federated identit*" OR "user-centric identit*" OR "user centric identit*" OR "self-sovereign identit*" OR "self sovereign identit*" OR „SSI" OR "digital twin*" OR "device identit*")* AND DOCUMENT TYPES: (Article) Indexes=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, BKCI-S, BKCI-SSH, ESCI, CCR-EXPANDED, IC Timespan=All years	1,010
Search terms 2: *TS=(("identit*") AND ("IOT" OR "internet of things*" OR "blockchain*" OR "block-chain*" OR "block chain*" OR "distributed ledg*" OR "DLT" OR "smart contract*" OR "smart-contract*"))* AND DOCUMENT TYPES: (Article) Indexes=SCI-EXPANDED, SSCI, A&HCI, CPCI-S, CPCI-SSH, BKCI-S, BKCI-SSH, ESCI, CCR-EXPANDED, IC Timespan=All years	495
Merging data sets (Removal of 53 duplicates)	1,452
Final data set (Removal of 57 unfitting articles after title and abstract screening)	1,395

2.2 Co-citation matrix and exploratory factor analysis

We use the secondary set of the 480 most-cited references to perform a co-citation analysis (or, more precisely, exploratory factor analysis and social network analysis). Co-citation analysis has been commonly used to identify intellectual structures of research environments (e.g. Ante, 2020a, 2020b; Ante et al., 2021; Wörfel, 2019; Zuschke, 2019).

One speaks of a co-citation when two articles refer to the same source. The underlying idea of co-citation analysis is that a common scientific basis of articles signals thematic proximity. Thus, if two articles have many common sources, i.e., many co-citations, it is likely that they are about the same (or a similar) topic. If an article in turn is cited by a large number of publications, i.e., has a high co-citation value, this indicates a high relevance of the article in a corresponding scientific discourse (Small, 1977, 1973).

For the purpose of the factor analysis and subsequent social network analysis, we obtain the co-citation matrix for the 480 most relevant references. The matrix is symmetric by definition. Each row and column represent one of the references, which results in a matrix whose cells show how often a publication was cited together with another publication. In line with the literature, the cells on the diagonal of the matrix do not show the co-citation value of a publication with itself, but rather the mean value of the corresponding column (McCain, 1990; Small, 1973). The co-citation matrix is obtained automatically through the Bibexcel software.

Explorative factor analysis is applied to identify underlying structures based on the relationships between variables. Assuming that a large number of co-citations mean similar ideas, theories and questions, we conclude that each identified factor represents a stream in

digital identity research. We identify factor loadings on the basis of principal component analysis. Factor loadings indicate how well an article fits into a factor, in our case how well a publication fits into a research stream. Factor loadings are essentially correlation coefficients. Thus, a factor loading of 0.7 and higher can be taken to indicate a good fit, whereas a loading higher than 0.4 indicates fit in general. (McCain, 1990). Results are rotated so that each variable is assigned the highest possible (-1 or 1) or lowest (0) value for the purpose of clearer differentiation. We calculate factor scores, which indicate how much a variable contributed to a factor by means of regression analysis. As regression coefficients, the factor scores signify the relevance of each publication to each research stream (DiStefano et al., 2009; Gorsuch, 1988; Nerur et al., 2008).

2.3 Keyword analysis and network analysis

We use the VOSviewer software to cluster and visualize keyword co-occurrences across publications. The software calculates the similarity between keywords based on co-occurrences and plots these as a network map. The similarity of keywords is visualized by the proximity of keywords on the network map. The software also computes clusters of similar keywords, displaying each cluster on the network map in a different colour (van Eck and Waltman, 2010).

The final step of the bibliometric analysis is a social network analysis. We use UCINET's NETDRAW companion program (Borgatti et al., 2002), which can map nodes based on geodesic distances (in our case the co-citation matrix). Nodes (individual publications) are be coloured (by research stream affiliation), connected with lines (indicating co-citations between articles) and adjusted in size (indicating overall number of co-citations). We thus obtain a map which illustrates the individual relevance of publications, the relationship between individual publications and the overarching research streams.

3 The scope of digital identity research

Section 3 first presents a mostly descriptive overview of the primary set of publications, which includes statistics on the number of publications per year, most relevant journals, highly-cited articles and research clusters based on keywords chosen by authors (Section 3.1). In Section 3.2, results of factor and social network analysis are described, which are based on the co-citation data. This includes an overview of identified research streams, brief subsections reviewing each stream, the visualization of stream interrelations and finally an overview of future research topics identified in the streams' publications.

3.1 Publishing trends

Figure 1 shows the number of publications per year from 1994 to 2019 for the primary set of 1,452 publications. One publication published in 1984 and articles published through January and April 2020 are not shown. The number of publications has increased steadily, with a steep increase in recent years. This underlines the increasing relevance of the topic.

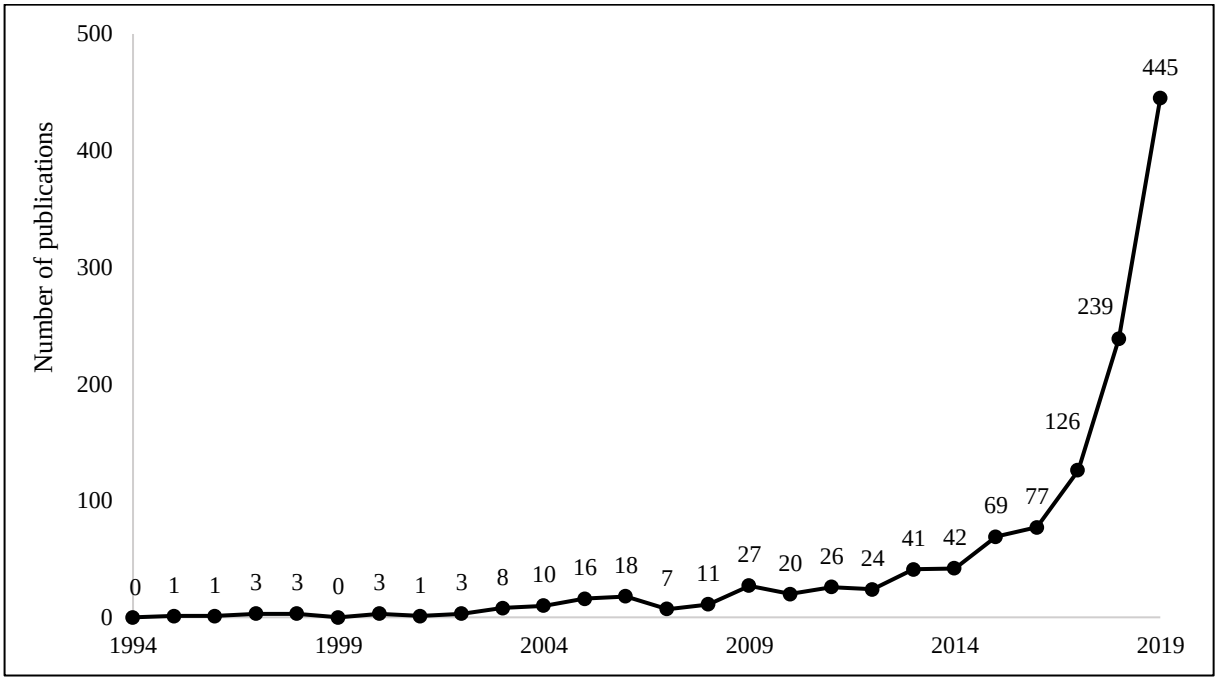

Figure 1. Number of publications per year in the primary set of publications on digital identity.

Table 2 shows the sources with the most publications and the number of publications by year. Most sources are computer science or engineering journals. With 87 publications, representing 6.2% of the total, IEEE Access is the journal with the highest number of publications. The first publications date back to 2016, after which the number of publications on the topic increases almost each year.

Table 3 shows the most-cited publications and their citation counts on Web of Science and Google Scholar. All of the articles were published in computer science or engineering journals.

Figure 2 shows the most frequently used author keywords (i.e. the keywords chosen by authors) in the 1,395 articles of the primary data set, clustered by co-occurrence. To ensure readability, only keywords with thirteen or more occurrences across all publications are shown. The software identifies four clusters. The first cluster contains the keywords Internet of Things (9.3%), security (8.0%) and authentication (5.9%). The second cluster contains the keywords digital twin (12.3%, the most frequently used keyword with 172 occurrences), smart manufacturing and Industry 4.0. The third contains the keyword blockchain (7.5%) and the fourth the keywords privacy (6.5%) and digital identity (6.1%).

Table 2. Top publishing sources for digital identity research by years of publication.

Source	Year of publication									Number of publications
	Before 2013	2013	2014	2015	2016	2017	2018	2019	2020 (Apr)	
IEEE Access					1	8	20	45	13	87
Sensors					1	2	4	15	8	30
IEEE Internet of Things Journal			5		2	1	4	15	3	30
Future Generation Computer Systems					1	3	13	9	2	28
ERCIM News					1	2	18	1		22
Security and Communication Networks	1		1	2	6		6	3		19
Applied Sciences					1		3	12	1	17
IEEE Transactions on Industrial Informatics						1	7	3	4	15
Wireless Personal Communications	4	2	1	1	1	2	3		1	15
Computer Law & Security Review	1	1	4	3	2	1	3			15
Computers & Security	2	1		1		1	2	4	4	15
International Journal of Computer Integrated Manufacturing								8	6	14
International Journal of Production Research								7	5	12
International Journal of Advanced Manufacturing Technology							4	4	3	11
Journal of Network and Computer Applications	1	1		1		1	4	3		11
Sustainability						1		4	6	11
IEEE Communications Magazine	4				1	1	2	3		11
ATP Edition						4	3	4		11
CIRP Annals – Manufacturing Technology						2	4	4		10
International Journal of Distributed Sensor Networks				1	1	1	2	4	1	10
Computer Networks	1	2	1	1	2			2		9
Robotics and Computer – Integrated Manufacturing								3	6	9
Digital Identity and Social Media		9								9
Total	14	16	12	10	20	31	102	153	63	421

Table 3. *Most-cited publications in digital identity research. Citation data was collected in April 2020.*

Publication	Title	Source	Times cited (Apr 2020)	
			Web of Science	Google scholar
Roman et al., 2013	On the features and challenges of security and privacy in distributed internet of things	Computer Networks	383	888
Kalnis et al., 2007	Preventing location-based identity inference in anonymous spatial queries	IEEE Transactions on Knowledge and Data Engineering	305	777
Yu et al., 2008	SybilGuard: Defending against sybil attacks via social networks	Computer Communication Review	206	1,003
Hossain and Muhammad, 2016	Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring	Computer Networks	206	377
Li et al., 2001	A remote password authentication scheme for multiserver architecture using neural networks	IEEE Transactions on Neural Networks	193	331
He et al., 2017	Anonymous Authentication for Wireless Body Area Networks with Provable Security	IEEE Systems Journal	180	261
Tao et al., 2018a	Digital twin-driven product design, manufacturing and service with big data	International Journal of Advanced Manufacturing Technology	175	458
Jain et al., 2004	Soft biometric traits for personal recognition systems	Biometric Authentication Proceedings	167	451
Cao et al., 2014	Displaced Dynamic Expression Regression for Real-time Facial Tracking and Animation	ACM Transactions on Graphics	144	267
Xue et al., 2013	A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks	Journal of Network and Computer Applications	140	233
Veletsianos, 2012	Higher education scholars' participation and practices on Twitter	Journal of Computer Assisted Learning	126	370
Bettini et al., 2005	Protecting privacy against location-based personal identification	Proceedings of Workshop on Secure Data Management	124	433
Wernke et al., 2014	A classification of location privacy attacks and approaches	Personal and Ubiquitous Computing	118	267
Sarma and Girão, 2009	Identities in the Future Internet of Things	Wireless Personal Communications	116	209
Kshetri, 2018	1 Blockchain’s roles in meeting key supply chain management objectives	International Journal of Information Management	114	384

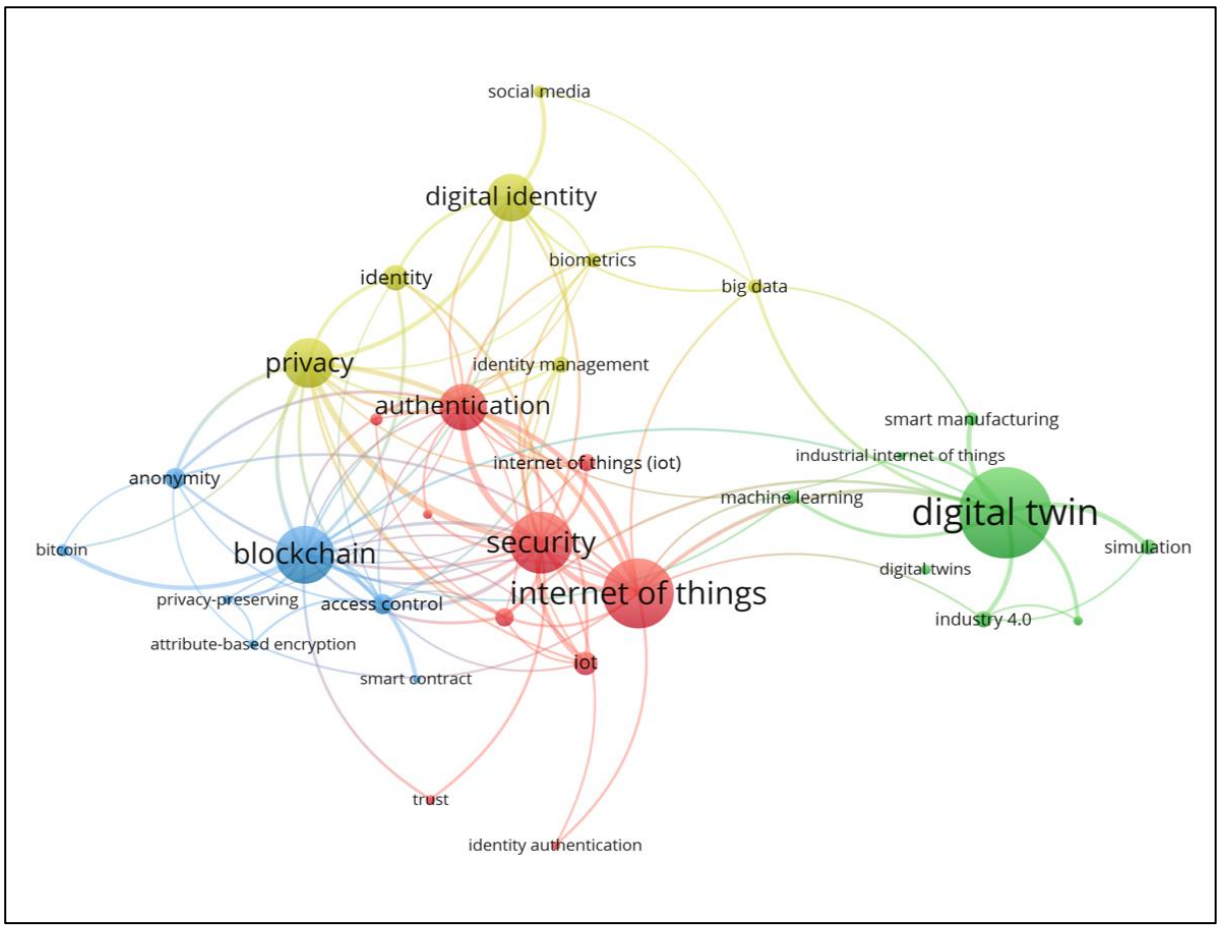

Figure 2. Co-occurrence of keywords. A minimal number of thirteen occurrences across publications is used as cutoff value. Node size illustrates the number of occurrences. The distance between nodes indicates the relatedness of the keywords, with co-occurrences being represented by lines between the nodes. Created with VOSviewer.

3.2 Research streams

Table 4 provides an overview of the seven identified research streams. We obtain a Kaiser-Meyer-Olkin (KMO) measure of 0.617 and a highly significant Bartlett test statistic, which suggests that explorative factor analysis via principal component analysis and Varimax rotation is a suitable approach for this data set. The final analysis is based on 453 articles, as 17 had to be excluded for statistical reasons. A share of 61.9% of publications can be assigned to at least one of the seven research streams. The research streams (i.e., the factors in the principal component analysis) only explain 36.4% of the variance, which indicates that research on digital identity is relatively heterogenous.

Figure 3 shows the relative and absolute prevalence of research streams over time, both per year and cumulated over time.

In the following subsections, each research stream is presented in detail.

Table 4. Overview of research streams in digital identity research.

Research stream	Explained variance	Share (all articles)	Share FL > 0.7 (in stream)	Main topics	Formative publications
I. Digital twin technology for smart manufacturing and industrial health monitoring	14.0%	25.8%	49.6%	- Introduction and overview of the digital twin concept - Requirements, challenges, benefits and guidelines for digital twin technology - Cyber-physical system prognostics and health monitoring (e.g., aircrafts, wind turbines, vehicles)	Tao et al. (2018a) Rosen et al. (2015)
II. Identity-based signcryption schemes	5.1%	7.1%	75.0%	- Identity-based signatures, encryption and signcryption schemes	Boyen (2003) Zheng (1999)
III. Distributed networks and user privacy	4.0%	6.0%	70.4%	- Technical foundations of distributed systems, peer-to-peer networks and blockchains - Extent of user privacy and anonymity in the Bitcoin network	Koshy et al. (2014) Nakamoto (2008)
IV. User authentication in wireless sensor networks	3.9%	7.7%	40.0%	- Authentication schemes in wireless sensor networks (e.g., BioHashing, elliptic curve cryptography) - Application-specific schemes (e.g., wireless body area networks (WBANs), telecare medical information systems (TMIS))	Das (2010) Turkanović et al. (2014)
V. Attribute-based encryption schemes	3.6%	6.0%	51.9%	- Attribute-based signatures and encryption schemes	Sahai and Waters (2005) Goyal et al. (2006)
VI. Secure data exchange in the Internet of Things	3.1%	4.4%	85.0%	- Security and privacy protection for data transmission - Data deduplication schemes - Secure data sharing and access control - Data moving and outsourcing encryption schemes	Shen et al (2018a) Li et al. (2018b)
VII. Blockchain and smart contracts for secure data management	2.7%	4.9%	45.5%	- Blockchain and smart contracts for secure and scalable data-driven applications, storage, sharing and management - Thematic focus on healthcare, medical and pharma sectors	Azaria et al. (2016) Yue et al. (2016)

FL: factor loading. Factor analysis is done via principal component analysis and Varimax rotation (43 iterations) with Kaiser normalization on the basis of 453 publications. KMO: 0.617; Bartlett test: $p < .001$.

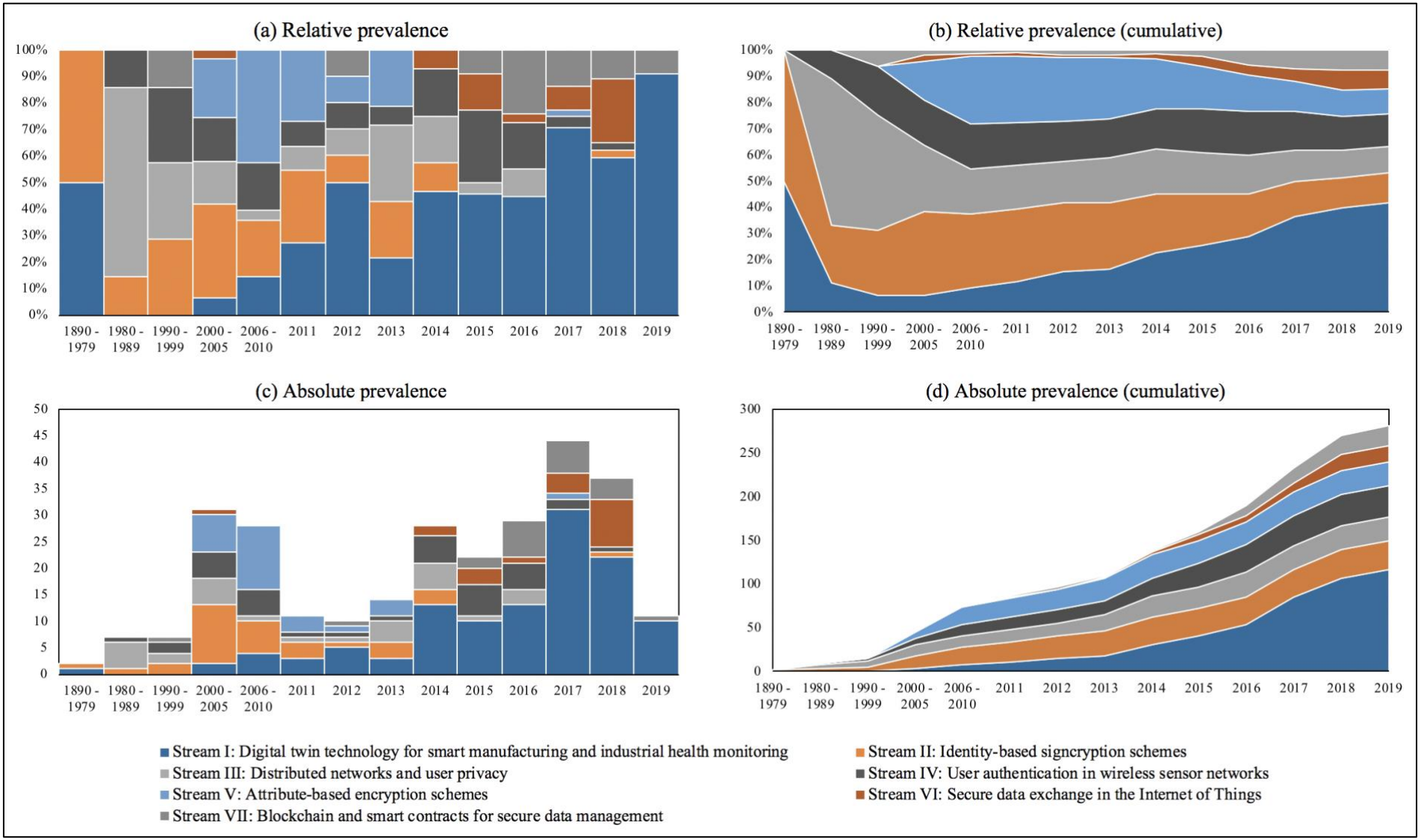

Figure 3. Relative and absolute prevalence of research stream affiliation by different time periods. Publications that are not assigned to one of the main research streams are omitted. Note the different sizes of time intervals on the x axis; these were chosen to avoid low observation counts in early periods.

3.2.1 Stream I: Digital twin technology for smart manufacturing and industrial health monitoring

The first stream comprises 25.8% of all publications, about half of which have a factor loading of 0.7 or higher. Overall, it explains 14% of variance in co-citations, making it the most relevant factor. As an overarching theme, the publications can be summarized under the collective term digital twin for smart manufacturing and industrial health monitoring. The earliest article of the stream was published in 2011 (Tuegel et al. 2011), revealing that Stream I is a relatively young field of research. Table 5 shows the fifteen publications with the highest factor loadings and the publication with the highest factor score in the stream.

Table 5. Key publications in Stream I: Digital twin technology for smart manufacturing and industrial health monitoring.

Publication	Factor loading	Factor score
Rosen et al., 2015	0.910	6.768
Schroeder et al., 2016	0.909	4.143
Uhlemann et al., 2017	0.904	3.277
Haag and Anderl, 2018	0.904	2.699
Canedo, 2016	0.902	2.195
Li et al., 2017	0.897	1.901
Grieves, 2014	0.896	1.997
Tao and Zhang, 2017	0.895	5.642
Negri et al., 2017	0.895	4.046
Glaessgen and Stargel, 2012	0.893	4.561
Schleich et al., 2017	0.892	5.936
Tao et al., 2018b	0.890	2.044
Gabor et al., 2016	0.889	2.540
Tuegel et al., 2011	0.886	3.423
Qi and Tao, 2018	0.880	3.746
…	…	…
Tao et al., 2018a	0.857	8.098
Other: 42 publications with FL > 0.7		

Digital twins are digital replicas of physical or digital objects, entities, processes, systems or devices. They provide connectivity for formerly non-connected processes, unification of data, programmability and automation, digital traceability and modularity (e.g. Tao et al., 2018a). In summary, the first stream considers how a meaningful connection between digital and physical systems can be created to improve the life cycle of objects.

The publication Tao et al. (2018a) has the highest factor score in Stream I. It discusses digital twin-driven products, manufacturing and big data. The authors describe a lack of convergence between products' digital and physical spaces, which results in low levels of design sustainability or efficiency. They propose a digital twin-based method for the design of products and illustrate three applications.

The publication with the highest factor loading and thus best overall fit in the stream is Rosen et al. (2015). It describes autonomous systems, digital twins and the future of manufacturing, pointing out that digital twins enable aligned systems which can combine real data with simulation data. The fact that the authors work for the company Siemens suggests that digital twins are an industry-driven development as much as an academic concept.

Multiple other studies in the stream provide an introduction to digital twins and their benefits, challenges and requirements for integration into production systems (Canedo, 2016; Gabor et al., 2016; Grieves, 2014; Haag and Anderl, 2018; Qi and Tao, 2018; Uhlemann et al., 2017).

Other studies focus on digital twin models, such as the open neutral data format AutomationML (Schroeder et al., 2016) or a novel shop-floor system (Tao and Zhang, 2017). The use of digital twins for prognostics and health management of cyber-physical systems is described for critical, high-value products such as aircraft wings (Li et al., 2017), aircraft structures (Tuegel et al., 2011), coming generations of NASA and U.S. Air Force vehicles (Glaessgen and Stargel, 2012) and wind turbines (Tao et al., 2018b).

3.2.2 Stream II: Identity-based signcryption

The second stream explains 5.08% of the variance and covers 7.1% of all publications. A proportion of 75% of publications with a factor loading of 0.7 or higher indicates a high homogeneity within the stream. Table 6 shows the fifteen publications with the highest factor loadings of Stream II.

Table 6. Key publications in Stream II: Identity-based signcryption.

Publication	Factor loading	Factor score
Chow et al., 2004	0.936	3.555
Gura et al., 2004	0.923	4.461
Roman and Lopez, 2009	0.910	5.120
Barreto et al., 2005	0.892	6.571
Boyen, 2003	0.881	5.153
Barbosa and Farshim, 2008	0.874	3.057
Oliveira et al., 2011	0.871	-0.502
Daemen and Rijmen, 2002	0.868	2.669
Shim, 2014	0.864	3.940
Cao et al., 2008	0.860	4.576
Li and Xiong, 2013	0.859	3.743
Zheng, 1999	0.854	6.122
Shim et al., 2013	0.851	4.552
Chen and Malone-Lee, 2005	0.840	2.567
Huang et al., 2011	0.824	2.836
Other: 13 publications with FL > 0.7		

Publications in the stream are concerned with identity-based signatures, encryption and signcryption models. Identity-based signatures are a form of public-key cryptography in which

a string represents information about a person or an object. A simple example of such information are email addresses as described by Shamir (1985) in the first implementation of identity-based signatures. In short, users on the internet can only verify digital signatures based on public information. The stream contains further ground-breaking cryptographic publications by Rivest et al. (1978) and Schnorr (1991), as well as the influential survey on the Internet of Things by Atzori et al. (2010).

Development of identity-based encryption schemes began in 2000 (Boneh and Franklin, 2003; Cocks, 2001). The term signcryption was introduced by Zheng (1999) to refer to the combination of digital signature and public key encryption in one step. Signcryption increases efficiency compared to processes which apply digital signatures before encryption.

Chow et al. (2004), the publication with the highest factor loading, proposes an identity-based encryption scheme, which enables public cyphertext authenticity. The authors motivate their work based on Boyen's (2003) first publicly verifiable and forward-secure identity-based encryption scheme that is provably secure and lacks the possibility for third parties to verify cyphertext.

Similarly, other publications in the stream introduce new identity-based signcryption models. Barreto et al. (2005), for example, introduce a model built upon bilinear maps that promises efficiency benefits. In Shim (2014), a pairing-free scheme is described, which promises computational efficiency and less overhead. Barbosa and Farshim (2008) describe certificateless signcryption. Cao et al. (2008) introduce a size-efficient pairing-free signature. An overarching theme of identity-based signcryption modelling are improvements in efficiency and security over existing schemes (Chen and Malone-Lee, 2005; Huang et al., 2011; Li and Xiong, 2013; Shim et al., 2013).

The publication Oliveira et al. (2011) combines a high thematic fit (factor loading) with a negative thematic relevance (factor score). It is concerned with pairing-based cryptography (PBC) in wireless networks, which – based on the statistical analysis – seems not very relevant for Stream II's thematic discourse (but can of course be highly relevant for other discourses).

Apart from identity-based signcryption models, the comparison between elliptic curve cryptography and the Rivest-Shamir-Adleman (RSA) algorithm (Gura et al., 2004), security analyses of sensor networks (Roman and Lopez, 2009) and the description of the Advanced Encryption Standard (also called Rijndael) (Daemen and Rijmen, 2002) are among the publications with the highest factor loadings.

3.2.3 Stream III: Distributed networks and user privacy

The third stream of research explains 4% of variance and comprises 6% of all publications. As over 70% of articles in the stream have a factor loading of 0.7 or higher, the discourse can be classified as relatively homogeneous. Research in this stream is concerned with distributed networks (such as blockchain or distributed ledger technology) and user privacy. The fifteen publications with the highest factor loadings and one publication with the highest factor score are shown in Table 7.

The Bitcoin whitepaper (Nakamoto, 2008) has the highest factor score but a relatively small factor loading. This suggests that Bitcoin serves as an important basis for research in this

stream but is rarely the actual research topic. Four of the fifteen publications shown in Table 7 describe basic technology or basic concepts on which blockchain builds, such as Merkle trees (Merkle, 1987) and Byzantine Fault Tolerance (Lamport et al., 1982). Two publications by Chaum (1981, 1983) lay out the technological foundations of privacy and anonymity on the internet. Dingledine et al. (2004) introduces the TOR network, an anonymous communication service.

Table 7. Key publications in Stream III: Distributed networks and user privacy.

Publication	Factor loading	Factor score
Bonneau et al., 2015	0.909	4.567
Reid and Harrigan, 2013	0.890	4.467
Koshy et al., 2014	0.877	6.697
Merkle, 1987	0.854	3.405
Lamport et al., 1982	0.853	3.130
Meiklejohn et al., 2013	0.828	5.408
Ron and Shamir, 2014	0.827	4.989
Dingledine et al., 2004	0.818	3.738
Androulaki et al., 2013	0.812	5.111
Narayanan et al., 2016	0.812	3.900
Chaum, 1981	0.800	3.759
Tschorsch and Scheuermann, 2016	0.788	4.553
Miers et al., 2013	0.780	4.452
Chaum, 1983	0.776	2.837
Ben-Sasson et al., 2014	0.773	5.338
…	…	…
Nakamoto, 2008	0.544	7.888
Other: 4 publications with FL > 0.7		

All other publications in the stream were published after the Bitcoin whitepaper and reference it. Bonneau et al. (2015) survey privacy-and anonymity-related topics of Bitcoin. Reid and Harrigan (2013) study the de-anonymization of Bitcoin users based on an alleged theft. Koshy et al. (2014) map Bitcoin addresses to IP addresses, concluding that their method allows them to tie about 1,000 Bitcoin addresses to their owners. Meiklejohn et al. (2013) analyse privacy and anonymity in the Bitcoin network by clustering wallet addresses. Ron and Shamir (2014) do so by studying the transaction graph, Androulaki et al., (2013) by simulating a Bitcoin-like system. Other studies provide technical introductions to blockchain technology and cryptocurrency (Narayanan et al., 2016; Tschorsch and Scheuermann, 2016). Lastly, two studies introduce privacy-centric cryptocurrencies: Zerocoin (Miers et al., 2013) and Zerocash (Ben-Sasson et al., 2014).

3.2.4 Stream IV: User authentication in wireless sensor networks

Stream four consists of 7.7% of all publications and explains 3.9% of variance. With only 40% of publications showing factor loadings of 0.70 or higher, research in the stream can be

classified as relatively heterogonous. The overarching topic of the research stream is user authentication in wireless sensor networks, mostly in the context of the Internet of Things. Table 8 shows factor loadings and factor scores of the fifteen most relevant publications.

Burrows et al. (1990) provide a formal overview of existing authentication protocols and suggest improvements. Their publication is the oldest in the research stream and can be considered a foundational publication for this stream's scientific discourse.

Das (2010), the study with the highest factor score and second highest factor loading, proposes a secure and efficient two-factor authentication scheme for wireless sensor networks. Khan and Alghathbar (2010) outline some security flaws in the scheme and warn against its use in real-world applications. They propose an improved scheme.

Table 8. Key publications in Stream IV: User authentication in wireless sensor networks.

Publication	Factor loading	Factor score
Lumini and Nanni, 2007	0.883	3.576
Das, 2010	0.853	6.681
Farash et al., 2016	0.853	4.666
Wang et al., 2015	0.832	2.854
Jin et al., 2004	0.828	3.695
Chang and Le, 2016	0.820	3.670
Khan and Alghathbar, 2010	0.817	3.757
Turkanović et al., 2014	0.794	6.319
Jiang et al., 2016	0.774	2.926
Choi et al., 2014	0.755	2.461
He et al., 2015	0.729	5.156
Xiong and Qin, 2015	0.717	2.837
Giri et al., 2015	0.715	2.351
He et al., 2015	0.711	2.903
Burrows et al., 1990	0.684	5.887

Jin et al. (2004) introduce BioHashing, a two-factor authentication through tokenized pseudo-random numbers and user fingerprints or other biometric characteristics. They argue that BioHashing is much more secure than simple biometrics. Lumini and Nanni (2007) suggest improvements to BioHashing to make data theft more difficult and improve performance in the event of theft.

Turkanović et al. (2014) propose an efficient user authentication scheme for wireless sensor networks based on simple cryptography, allowing users to authenticate a sensor without having to communicate with a specific system. Subsequent studies outline potential vulnerabilities of the scheme and suggest improvements: These include impersonation attacks, stolen smart card attacks and spoofing attacks (Chang and Le, 2016) as well as cryptographic attacks (Farash et al., 2016).

Other studies propose improvements to authentication schemes through three-factor elliptic curve cryptography (Jiang et al., 2016), user authentication via elliptic curve cryptography

(Jiang et al., 2016) and a temporal-credential-based mutual authentication and key agreement scheme (He et al., 2015). Wang et al. (2015) propose an evaluation metric for practicable, anonymous two-factor authentication schemes.

He et al. (2015) review anonymous authentication schemes for the exchange of medical data in wireless body area networks (WBANs) which connect wearable computing devices on the clothes, the skin or in the body of humans. Xiong and Qin (2015) discuss certificateless signatures in WBANs. Medical data is also at the centre of the study Giri et al. (2015), who describe password risks in an authentication scheme for telecare medical information systems (TMISs) proposed by Khan and Kumari (2013) and propose an improved version of the scheme.

3.2.5 Stream V: Attribute-based encryption

The fifth research stream explains 3% of variance and consists of 4.4% of all publications. As 85% of the publications under consideration have factor loadings of 0.7 or higher, the stream can be classified as highly homogenous, which is likely due to the frequent appearance of the same authors. Research in the stream deals with attribute-based encryption. Compared to identity-based encryption (Stream II), where users are identified on the basis of a unique identifier (such as a username), attribute-based encryption partially identifies users through various attributes (such as the user's location). Only if these attributes match, ciphertext can be decrypted. All publications with factor loadings of 0.7 and higher are shown in Table 9.

Table 9. Key publications in Stream V: Attribute-based encryption.

Publication	Factor loading	Factor score
Waters, 2011	0.897	4.059
Ostrovsky et al., 2007	0.894	0.288
Chase, 2007	0.887	4.600
Chase and Chow, 2009	0.863	4.145
Lewko and Waters, 2011	0.860	3.080
Emura et al., 2009	0.850	3.787
Lewko et al., 2010	0.828	4.144
Bethencourt et al., 2007	0.810	7.276
Sahai and Waters, 2005	0.808	9.403
Rouselakis and Waters, 2013	0.796	2.080
Goyal et al., 2006	0.748	10.481
M. Li et al., 2013	0.743	2.596
Yu et al., 2010	0.742	1.915
Li et al., 2010	0.700	1.868

Sahai and Waters (2005) and Goyal et al. (2006) initially proposed attribute-based authentication. Their high factor scores (9.40 and 10.48) attest their high relevance for the stream's scientific discourse.

Various other studies in the stream build on these studies, proposing improvements with regard to multi-authorities (Chase, 2007), downstream related privacy and security (Chase and Chow, 2009), decentralization (Lewko and Waters, 2011), private key expression (Ostrovsky et al., 2007), new signature signing techniques (Li et al., 2010), fully secure attribute-based encryption and attribute-hiding predicate encryption (Lewko et al., 2010) and large-universe approaches (Rouselakis and Waters, 2013).

The approach by Goyal et al. (2006) can be classified as key-policy attribute-based encryption (KP-ABE), where user keys are generated through an access tree of user privileges and encryption occurs over attributes. An alternative approach is cyphertext-policy attribute-based encryption (CP-ABE), where access trees are used to encrypt data and the secret keys of users are generated over attributes (Bethencourt et al., 2007; Emura et al., 2009; Waters, 2011).

Lastly, two studies address attribute-based authentication in specific areas of application: cloud computing (Yu et al., 2010) and personal health records (M. Li et al., 2013).

3.2.6 Stream VI: Secure data exchange in the Internet of Things

Stream VI deals with the secure and anonymous exchange of data in the Internet of Things, especially in cloud computing. It includes 4.4% of all publications. With 85% of publications having factor loadings of 0.7 and higher, it is the stream with the highest homogeneity – probably because the same authors often appear. Overall, the stream explains 3% of variance in co-citations. Table 10 shows the fifteen articles with the highest factor loadings.

Table 10. Key publications in Stream VI: Secure data exchange in the Internet of Things.

Publication	Factor loading	Factor score
Shen et al., 2018a	0.887	5.780
J. Li et al., 2013	0.876	4.748
Xu et al., 2018	0.866	5.651
Li et al., 2015a	0.859	4.215
Cai et al., 2017	0.856	5.552
Y. Zhang et al., 2018	0.855	5.105
Li et al., 2018b	0.849	6.665
Shen et al., 2018c	0.828	5.470
Zhang et al., 2016	0.820	4.350
Li et al., 2014	0.815	4.308
Huang et al., 2017	0.810	3.564
Li et al., 2018a	0.783	3.471
Shen et al., 2018b	0.776	3.876
Li et al., 2015c	0.774	6.492
Li et al., 2015b	0.759	4.352
Other: 1 publication with FL > 0.7		

A recurring topic is attribute-based encryption, which was identified as the overarching theme of Stream V. While studies in Stream V focus on basic methods and schemes, studies in Stream

VI consider the application of attribute-based encryption in the context of mobile devices and cloud computing. Li et al. (2018b), the study with the highest factor score, points out that attribute-based encryption suffers from high computation cost and low security and proposes an improved data-sharing scheme for mobile devices in cloud computing networks. The study with the second largest factor score also builds on attribute-based encryption and introduces outsourcing computation (Li et al., 2015c). This is also the topic of J. Li et al. (2013). Li et al. (2018a) propose a privacy-aware multi-authority ciphertext-policy scheme which hides attribute information in the ciphertext.

Shen et al. (2018a) propose a secure scheme for uploading data in home area networks (HANs). It ensures integrity of data by prohibiting malicious home gateways from modifying it. Other application-specific publications consider the flexible sharing of electronic health records with offline encryption and outsourced decryption (Cai et al., 2017), a privacy-aware health data access control system with partially hidden access policies (Y. Zhang et al., 2018) and anonymous, certificateless, cloud-aided authentication in WBANs

Other topics include homomorphic encryption (Xu et al., 2018), a match-then-decrypt scheme (Zhang et al., 2016), selective opening security (Huang et al., 2017), data deduplication (Li et al., 2015a) and anonymous but traceable data sharing (Shen et al., 2018b).

3.2.7 Stream VII: Blockchain and smart contracts for secure data management

The seventh research stream consists of 4.9% of the articles and explains 2.7% of variance. A share of 46% of articles in the stream have factor loadings of 0.7 or higher. Studies in this stream consider how blockchain and smart contracts can enable the secure storage, management and exchange of data, especially high-risk healthcare and medical data. The stream's ten articles with factor loadings higher than 0.7 are shown in Table 11. Additionally, the Bitcoin whitepaper (Nakamoto, 2008) as its high factor score indicates a high thematic relevance for the stream. While its factor loading of 0.401 would justify assignment to Stream VII, it has a higher factor score for Stream III (cf. Table 7) and thus assigned to the latter.

The article of Shae and Tsai (2017) describes a blockchain architecture for data from clinical trials and precision medicine. Other highly relevant studies in the stream also consider the use of blockchain for secure and scalable clinical data, medical records or pharma supply-chains (Azaria et al., 2016; Bocek et al., 2017; Dubovitskaya et al., 2017; Xia et al., 2017; Yue et al., 2016; P. Zhang et al., 2018). The study by Kuo et al. (2017) reviews previous research on blockchain in the context of biomedical and healthcare applications. Accordingly, it has a high thematic fit (indicated by a high factor loading) but low relevance for the stream's academic discourse (as indicated by a negative factor score).

Other publications in the stream focus more generally on smart contracts. Luu et al. (2016) study the security of smart contracts on the Ethereum blockchain, Delmolino et al. (2016) discuss the design and deployment of smart contracts.

Table 11. Key publications in Stream VII: Blockchain and smart contracts for secure data management.

Publication	Factor loading	Factor score
Shae and Tsai, 2017	0.856	4.758
P. Zhang et al., 2018	0.846	5.370
Dubovitskaya et al., 2017	0.836	3.504
Kuo et al., 2017	0.828	-0.305
Delmolino et al., 2016	0.822	4.575
Luu et al., 2016	0.779	4.458
Yue et al., 2016	0.776	6.257
Azaria et al., 2016	0.760	8.681
Bocek et al., 2017	0.716	3.254
Xia et al., 2017	0.705	4.301
…	…	…
Nakamoto, 2008	0.401	8.252

3.3 Interrelations of research streams

Figure 4 shows the results of the social network analysis. Every node in the network represents one publication, whereby for clarity only the first author and the year of publication are shown. Connections between publications signal co-citations, while the size of a node represents how often a publication is co-cited. The colour coding indicates to which of the seven research streams a publication can be assigned - or in the case of grey nodes whether a publication can be assigned to any of the seven streams described above.

One important finding of the network analysis is that Stream I has few connections to other streams, with essential links only existing to Streams II and VII. This independently confirms a similar finding in the keyword analysis, which was based on the primary data set. The other streams share stronger relationships or even overlap. The two research streams centred on encryption, Streams II and V, are located in the middle of the research network as basic technologies and exhibit a high degree of overlap.

3.4 Recommendations for future research

This section summarizes recommendations for future research mentioned in the high-impact publications presented in Tables 5 through 11, based on manual inspection of the articles. To provide a structured overview, we cluster research topics within each stream. Table 12 summarizes the recommendations.

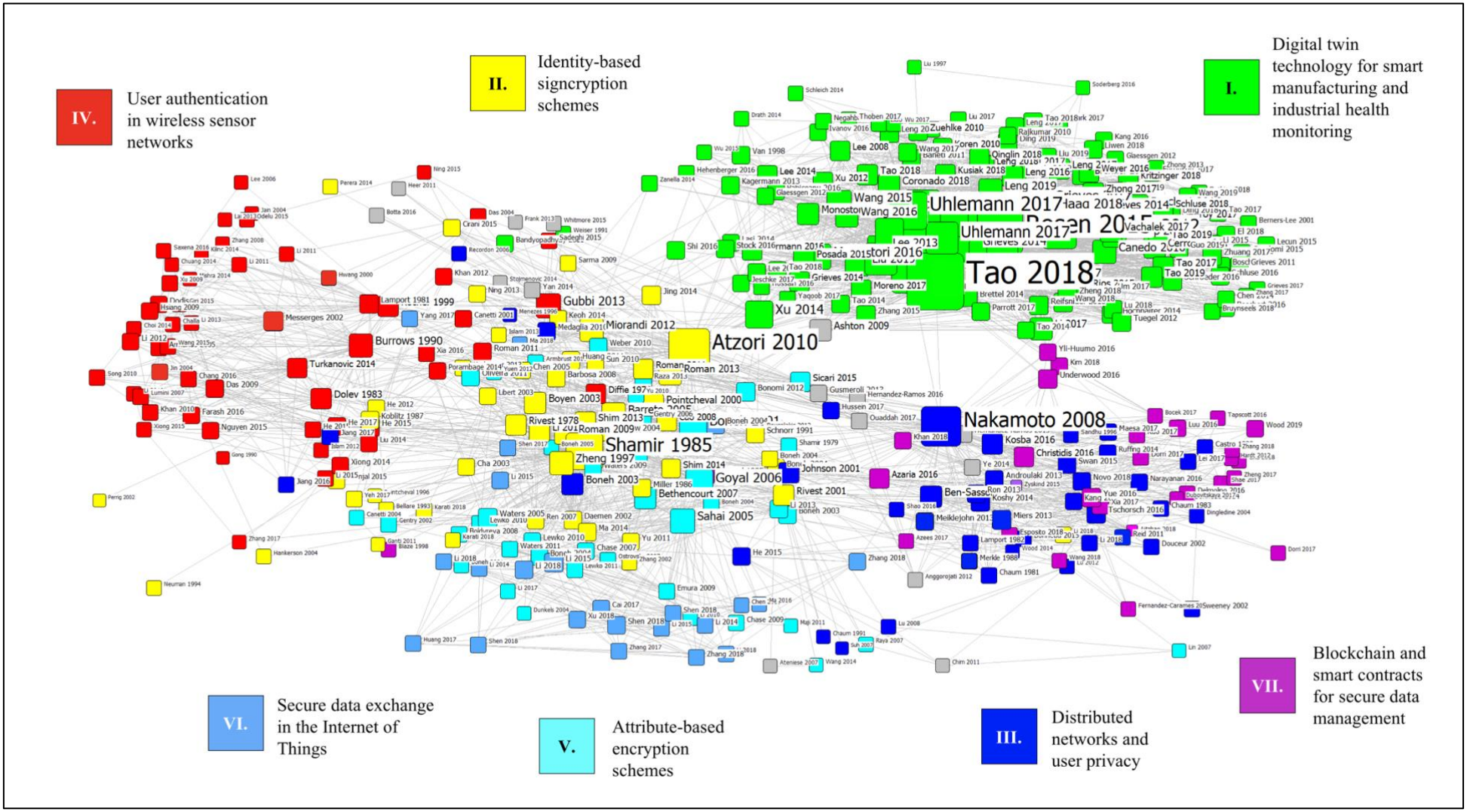

Figure 4. Results of the social network analysis. Each node represents a publication. For readability, only the first author is displayed. Node colour shows the most relevant research stream based on factor loading, with grey nodes not belonging to any of the seven streams. Node size represents the absolute number of co-citations, lines between articles represent the number of co-citations. Created with UCINET software. A high-resolution version is available online at https://dx.doi.org/10.17632/9htchvnnd4.1.

Table 12. Recommended topics for future research mentioned in high-impact publications.

Research stream	Future research topics
I. Digital twin technology for smart manufacturing and industrial health monitoring	- Interconnection and interaction (Tao and Zhang, 2017; Tao et al., 2018a; Qi and Tao, 2018; Schroeder et al., 2016; Negri et al., 2017; Uhlemann et al., 2017) - Integration in development process and life cycle (Haag and Anderl, 2018; Gabor et al., 2016; Tao et al., 2018a) - Smart analytics of digital twin data (Tao et al., 2018a; Haag and Anderl, 2018) - Industrial applications (Negri et al., 2017; Tao and Zhang, 2017; Qi and Tao, 2018)
II. Identity-based signcryption schemes	- Security protocols for small devices (Gura et al., 2004) - Authentication schemes (Cao et al., 2008) - Signcryption & public key cryptosystems (Zheng, 1999) - Heterogeneous signcryption (Huang et al., 2011)
III. Distributed networks and user privacy	- Cryptocurrency (Tschorsch and Scheuermann, 2016; Bonneau et al., 2015; Miers et al., 2013). - Privacy-preserving verification and enforcement (Ben-Sasson et al., 2014) - Tor network (Dingledine et al., 2004) - Public-key cryptography (Miers et al., 2013)
IV. User authentication in wireless sensor networks	- BioHashing (Lumini and Nanni, 2007) - Fuzzy verifiers (Wang et al., 2015) - Secure mobile cloud computing (He et al., 2015) - Remote authentication & revocation (Xiong and Qin, 2015)
V. Attribute-based encryption schemes	- New attribute-based encryption systems (Bethencourt et al., 2007) - Identity-based encryption (Sahai and Waters, 2005)
VI. Secure data exchange in the Internet of Things	- Standardization for shared (clinical) data (Shen et al., 2018a; Y. Zhang et al., 2018; Li et al., 2018b; Shen et al., 2018c) - Encryption (Zhang et al., 2016; Li et al., 2015b)
VII. Blockchain and smart contracts for secure data management	- Mining (Azaria et al., 2016) - Connected health and medical data (Dubovitskaya et al., 2017) - Privacy-preserving health data (P. Zhang et al., 2018).

Stream I's high-impact literature suggests four areas for future research. The first is interconnection and interaction of digital twin technology (Tao and Zhang, 2017; Tao et al., 2018a; Qi and Tao, 2018; Schroeder et al., 2016; Negri et al., 2017; Uhlemann et al., 2017). Tao and Zhang (2017) see potential for further investigations into the two-way connection between physical and virtual spaces. Uhlemann et al. (2017) note the need for more research on production using cyber-physical systems in medium-sized enterprises. The second proposed area of research is the integration of digital twin technology into the development process and the overall life cycle of systems and products (Haag and Anderl, 2018; Tao et al., 2018a; Gabor

et al., 2016). Haag and Anderl (2018) mention digital twin automation and its implementation and communication with the physical replica. Gabor et al. (2016) ask how digital twins can best be integrated into the development process and the overall system life cycle. The third area is concerned with smart analytics of digital twin data (Tao et al., 2018a; Haag and Anderl, 2018). Haag and Anderl (2018) suggest that digital twins require a new approach to how data are collected and processed. Finally, actual (industrial) applications of digital twin need further research (Negri et al., 2017; Tao and Zhang, 2017; Qi and Tao, 2018). For example, Negri et al. (2017) call for investigations into and demonstrations of the wide range of applications and benefits of digital twins.

The future research identified within Stream II comes from articles published between 2004 and 2011. Hence it is likely that these topics have already developed further. Nonetheless, these recommendations show what highly influential researchers felt was relevant at the time of publication. Again, we identify four areas: 1) Security protocols for small devices, such as lightweight SSL/TLS implementations (Gura et al., 2004), 2) authentication schemes, such as identity-based multi-user broadcast authentication on TinyOS (Cao et al., 2008), 3) signcryption and public key cryptosystems employing RSA or other public key cryptosystems (Zheng, 1999) and 4) heterogeneous signcryption which would, for example, enable users to receive ciphertext (Huang et al., 2011).

Stream III's topics for future research can be clustered as: 1) Research on cryptocurrencies (Bitcoin and "altcoins"), especially with regard to privacy and the use of anonymous credentials (Bonneau et al., 2015; Miers et al., 2013), 2) privacy-preserving verification and enforcement, including policy-related questions (Ben-Sasson et al., 2014), 3) research on the Tor network, such as its scalability, bandwidth classes, incentives and approaches to limiting abuse (Dingledine et al., 2004), and 4) research on public-key cryptography (Miers et al., 2013).

For Stream IV, we identify: 1) BioHashing and its extension to other biometric characteristics, such as the iris (Lumini and Nanni, 2007), 2) fuzzy verifiers, which should be evaluated further for practical effectiveness (Wang et al., 2015), 3) the security of mobile cloud computing (He et al., 2015) and 4) remote authentication and revocation (Xiong and Qin, 2015).

Stream V's future research topics can be divided into two areas: 1) Novel attribute-based encryption systems, for example systems with different types of expressibility (Bethencourt et al., 2007) and 2) identity-based encryption, which could include different distance metrics between identities (Sahai and Waters, 2005).

Future research mentioned in Stream VI can be clustered in two groups: 1) Design of a searchable and verifiable data upload scheme as part of a standard for sharing of clinical data (Shen et al., 2018a;Y. Zhang et al., 2018; Li et al., 2018b; Shen et al., 2018c) and 2) encryption (Zhang et al., 2016; Li et al., 2015b), including the construction of more expressive and fully secure anonymous schemes (Zhang et al., 2016).

High-impact publications in Stream VII recommend further research into 1) "Mining" related to medical research (Azaria et al., 2016), 2) the connection of health and medical data to enhance healthcare data management (Dubovitskaya et al., 2017) and 3) the construction of privacy-preserving and secure health systems (P. Zhang et al., 2018).

4 Concluding remarks

This study analyses research on digital identity against the background of new markets and technologies such as the Internet of Things or blockchain technology. To screen the existing research in a systematic and empirical way, we employ various bibliometric research methods. We observe that the number of publications on digital identity has grown exponentially during the last few years. The majority of publications comes from computer science and engineering. This suggests that digital identity is experiencing a surge of interest but that the underlying technologies are far from mature. We list the most active journals and most-cited publications in the field. In addition, an analysis of author keywords reveals that so far research has largely focused on theoretical concepts and technical issues – with the exception of research into the application of digital twin technology.

We apply explorative factor analysis to co-citation data to identify research streams within the field. Our analysis identifies seven research streams, which we name: i) Digital twin technology for smart manufacturing and industrial health monitoring, ii) identity-based signcryption schemes, iii) distributed networks and user privacy, iv) user authentication in wireless sensor networks, v) attribute-based encryption schemes, vi) secure data exchange in the Internet of Things and vii) blockchain and smart contracts for secure data management. Streams II, IV and V are concerned with encryption and authentication. Streams III, IV and VII also comprise highly technical publications, though on more overarching themes such as distributed networks, secure data exchange and blockchain technology. We present the key publications for each research stream and analyse the interrelations of research streams and their evolution over time. In addition, we extract recommendations for future research from each stream's key publications and cluster them for easy reference.

The only keyword from an application domain is "digital twin". Research on digital twin appears to still be in its infancy, which is underlined by the frequent occurrence of the keyword "simulation" in this cluster. This is unsurprising since renewed interest was arguably only sparked by the relatively recent publication of Grieves (2014) – although one could argue that similar ideas were already pursued much earlier, e.g., when NASA mirrored systems in space missions (Glaessgen and Stargel, 2012). The great relevance of digital twin for digital identity research is one of the main findings of this study. At the same time, the social network analysis shows that the research stream on digital twins and related concepts such as smart manufacturing and Industry 4.0 (Stream I) is mostly detached from the other research streams. Strengthening these connections might yield promising research results.

Our results illustrate that digital identity research is still in its infancy but is evolving fast. Dominant technologies and frameworks have yet to emerge. Fundamental questions and technical issues around privacy and security continue to engage researchers. At the same time, research on digital twins is pushing innovation in digital identity with a stronger focus on application and realizable use cases. We observe, however, that the more technical research streams share little overlap with the research stream on digital twins and suggest that bridging this gap could benefit the entire field of digital identity research.

We hope that our systematic and comprehensive literature review can serve to identify and differentiate the many research topics in the field of digital identity. It can assist researchers in

keeping track of this young and fast-growing research area, reduce search costs and highlight worthwhile avenues for future research. The internet may have been built without an identity layer – but researchers are working hard to change that.

References

Allen, C., 2016. The Path to Self-Sovereign Identity [WWW Document]. URL http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed 7.4.20).

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating User Privacy in Bitcoin, in: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, pp. 34–51.

Ante, L., 2020a. Smart Contracts on the Blockchain – A Bibliometric Analysis and Review. Telemat. Informatics. https://doi.org/10.1016/j.tele.2020.101519

Ante, L., 2020b. A place next to Satoshi: scientific foundations of blockchain and cryptocurrency in business and economics. Scientometrics 124, 1305–1333. https://doi.org/10.1007/s11192-020-03492-8

Ante, L., Steinmetz, F., Fiedler, I., 2021. Blockchain and energy: A bibliometric analysis and review. Renew. Sustain. Energy Rev. 137, 110597. https://doi.org/10.1016/j.rser.2020.110597

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of Things: A survey. Comput. Networks 54, 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. MedRec: Using Blockchain for Medical Data Access and Permission Management. https://doi.org/10.1109/OBD.2016.11

Barbosa, M., Farshim, P., 2008. Certificateless signcryption, in: Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security, ASIACCS '08. pp. 369–372. https://doi.org/10.1145/1368310.1368364

Barreto, P.S.L.M., Libert, B., McCullagh, N., Quisquater, J.J., 2005. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 515–532. https://doi.org/10.1007/11593447_28

Bazarhanova, A., Smolander, K., 2020. The Review of Non-Technical Assumptions in Digital Identity Architectures. Proc. 53rd Hawaii Int. Conf. Syst. Sci. 3, 6408–6417. https://doi.org/10.24251/hicss.2020.785

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., 2014. Zerocash: Decentralized anonymous payments from bitcoin. Proc. - IEEE Symp. Secur. Priv. 459–474. https://doi.org/10.1109/SP.2014.36

Bethencourt, J., Sahai, A., Waters, B., 2007. Ciphertext-policy attribute-based encryption, in: IEEE Symposium on Security and Privacy (SP'07). IEEE, pp. 321–334. https://doi.org/10.1007/978-3-319-04873-4_12

Bettini, C., Wang, X.S., Jajodia, S., 2005. Protecting privacy against location-based personal identification, in: Thuraisingham, B. (Ed.), Secure Data Management. Springer, Berlin, Heidelberg, pp. 361–375. https://doi.org/10.1201/9781420013221.axb

Blue, J., Condell, J., Lunney, T., 2018. A Review of Identity, Identification and Authentication. Int. J. Inf. Secur. Res. 8, 794–804. https://doi.org/10.20533/ijisr.2042.4639.2018.0091

Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B., 2017. Blockchains Everywhere - A Use-case of Blockchains in the Pharma Supply-Chain, in: 2017 IFIP/IEEE Symposium on Integrated Network and Service Management. IEEE, pp. 772–777. https://doi.org/10.23919/INM.2017.7987376

Boneh, D., Franklin, M., 2003. Identity-based encryption from the weil pairing. SIAM J. Comput. 32, 586–615. https://doi.org/10.1137/S0097539701398521

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W., 2015. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. Proc. - IEEE Symp. Secur. Priv. 2015-July, 104–121. https://doi.org/10.1109/SP.2015.14

Borgatti, S.P., Everett, M.G., Freeman, L.C., 2002. Ucinet for Windows: Software for social network analysis. Harvard MA Anal. Technol. 6.

Boyen, X., 2003. Multipurpose Identity-Based Signcryption - A Swiss Army Knife for Identity-Based

Cryptography, in: Advances in Cryptology - CRYPTO 2003. pp. 383–399. https://doi.org/10.1007/b11817

Burrows, M., Abadi, M., Needham, R., 1990. A logic of Authentication. ACM Trans. Comput. Syst. 8, 18–36. https://doi.org/10.1145/77648.77649

Cai, Z., Yan, H., Li, P., Huang, Z. an, Gao, C., 2017. Towards secure and flexible EHR sharing in mobile health cloud under static assumptions. Cluster Comput. 20, 2415–2422. https://doi.org/10.1007/s10586-017-0796-5

Cameron, K., 2005. The Laws of Identity. Microsoft Corp 8–11.

Canedo, A., 2016. Industrial IoT lifecycle via digital twins, in: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis. pp. 1–1. https://doi.org/10.1145/2968456.2974007

Cao, C., Hou, Q., Zhou, K., 2014. Displaced dynamic expression regression for real-time facial tracking and animation. ACM Trans. Graph. 33. https://doi.org/10.1145/2601097.2601204

Cao, X., Kou, W., Dang, L., Zhao, B., 2008. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. Comput. Commun. 31, 659–667. https://doi.org/10.1016/j.comcom.2007.10.017

Chang, C.C., Le, H.D., 2016. A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks. IEEE Trans. Wirel. Commun. 15, 357–366. https://doi.org/10.1109/TWC.2015.2473165

Chase, M., 2007. Multi-authority attribute based encryption, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 515–534. https://doi.org/10.1007/978-3-540-70936-7_28

Chase, M., Chow, S.S.M., 2009. Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing, in: IEEE Access. pp. 121–130.

Chaum, D., 1983. Blind signatures for untraceable payments, in: Advances in Cryptology. Springer Boston, MA, pp. 199–203.

Chaum, D.L., 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Commun. ACM 24, 84–90. https://doi.org/10.1145/358549.358563

Chen, L., Malone-Lee, J., 2005. Improved Identity-Based Signcryption, in: International Workshop on Public Key Cryptography. Springer Berlin Heidelberg, pp. 362–379.

Chen, Y., Leimkuhler, F.F., 1986. A relationship between Lotka's Law, Bradford's Law, and Zipf's Law. J. Am. Soc. Inf. Sci. 37, 307–314.

Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., Won, D., 2014. Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors (Switzerland) 14, 10081–10106. https://doi.org/10.3390/s140610081

Chow, S.S.M., Yiu, S.M., Chow, L.C.K., Chow, K.P., 2004. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity, in: Lecture Notes in Computer Science 2971.

Cocks, C., 2001. An identity based encryption scheme based on quadratic residues. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 2260, 360–363. https://doi.org/10.1007/3-540-45325-3_32

Daemen, J., Rijmen, V., 2002. AES the advanced encryption standard 1–238.

Das, M.L., 2010. Improved two-factor user authentication in wireless sensor networks, in: 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob'2010. pp. 600–606. https://doi.org/10.1109/WIMOB.2010.5645004

Delmolino, K., Arnett, M., Kosba, A., Miller, A., Shi, E., 2016. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. Lect. Notes Comput. Sci. 79–94. https://doi.org/10.1007/978-3-662-53357-4_6

Dingledine, R., Mathewson, N., Syverson, P., 2004. Tor - the second-generation onion router. Usenix Secur. 303–320.

DiStefano, C., Zhu, M., Mîndrilă, D., 2009. Understanding and using factor scores: Considerations for the applied researcher. Pract. Assessment, Res. Eval. 14.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., Wang, F., 2017. Secure and Trustable Electronic

Medical Records Sharing using Blockchain, in: AMIA Annual Symposium Proceedings. pp. 650–659.

Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M., 2009. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length, in: International Conference on Information Security Practice and Experienc. Springer, Berlin, Heidelberg, p. 13.23.

Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks 36, 152–176. https://doi.org/10.1016/j.adhoc.2015.05.014

Ferdous, M.S., Chowdhury, F., Alassafi, M.O., 2019. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access 7, 103059–103079. https://doi.org/10.1109/access.2019.2931173

Gabor, T., Belzner, L., Kiermeier, M., Beck, M.T., Neitz, A., 2016. A simulation-based architecture for smart cyber-physical systems, in: Proceedings - 2016 IEEE International Conference on Autonomic Computing, ICAC 2016. pp. 374–379. https://doi.org/10.1109/ICAC.2016.29

Giri, D., Maitra, T., Amin, R., Srivastava, P.D., 2015. An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems. J. Med. Syst. 39. https://doi.org/10.1007/s10916-014-0145-7

Glaessgen, E.H., Stargel, D.S., 2012. The digital twin paradigm for future NASA and U.S. Air force vehicles. Collect. Tech. Pap. - AIAA/ASME/ASCE/AHS/ASC Struct. Struct. Dyn. Mater. Conf. https://doi.org/10.2514/6.2012-1818

Gorsuch, R.L., 1988. Exploratory Factor Analysis, in: Nesselroade, J.R., Cattell, R.B. (Eds.), Handbook of Multivariate Experimental Psychology. Springer US, Boston, MA, pp. 231–258. https://doi.org/10.1007/978-1-4613-0893-5_6

Goyal, V., Pandey, O., Sahai, A., Waters, B., 2006. Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the ACM Conference on Computer and Communications Security. pp. 89–98. https://doi.org/10.1145/1180405.1180418

Grieves, M., 2014. Digital Twin: Manufacturing Excellence through Virtual Factory Replication.

Gura, N., Patel, A., Wander, A., Eberle, H., Shantz, S.C., 2004. Comparing elliptic curve cryptography and RSA on 8-Bit CPUs. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 3156, 119–132. https://doi.org/10.1007/978-3-540-28632-5_9

Haag, S., Anderl, R., 2018. Digital twin – Proof of concept. Manuf. Lett. 15, 64–66. https://doi.org/10.1016/j.mfglet.2018.02.006

He, D., Kumar, N., Chilamkurti, N., 2015. A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. Inf. Sci. (Ny). 321, 263–277. https://doi.org/10.1016/j.ins.2015.02.010

He, D., Zeadally, S., Kumar, N., Lee, J.H., 2017. Anonymous Authentication for Wireless Body Area Networks with Provable Security. IEEE Syst. J. 11, 2590–2601. https://doi.org/10.1109/JSYST.2016.2544805

Hossain, M.S., Muhammad, G., 2016. Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring. Comput. Networks 101, 192–202. https://doi.org/10.1016/j.comnet.2016.01.009

Houtan, B., Hafid, A.S., Makrakis, D., 2020. A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. IEEE Access 8, 90478–90494. https://doi.org/10.1109/ACCESS.2020.2994090

Huang, Q., Wong, D.S., Yang, G., 2011. Heterogeneous signcryption with key privacy. Comput. J. 54, 525–536. https://doi.org/10.1093/comjnl/bxq095

Huang, Z., Liu, S., Mao, X., Chen, K., Li, J., 2017. Insight of the protection for data security under selective opening attacks. Inf. Sci. (Ny). 412–413, 223–241. https://doi.org/10.1016/j.ins.2017.05.031

Jain, A.K., Dass, S.C., Nandakumar, K., 2004. Soft biometric traits for personal recognition systems. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 3072, 731–738. https://doi.org/10.1007/978-3-540-25948-0_99

Jiang, Q., Khan, M.K., Lu, X., Ma, J., He, D., 2016. A privacy preserving three-factor authentication protocol for e-Health clouds. J. Supercomput. 72, 3826–3849. https://doi.org/10.1007/s11227-015-1610-x

Jin, A.T.B., Ling, D.N.C., Goh, A., 2004. Biohashing: Two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit. 37, 2245–2255. https://doi.org/10.1016/j.patcog.2004.04.011

Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D., 2007. Preventing location-based identity inference in anonymous spatial queries. IEEE Trans. Knowl. Data Eng. 19, 1719–1733. https://doi.org/10.1109/TKDE.2007.190662

Khan, M.K., Alghathbar, K., 2010. Cryptanalysis and security improvements of "two-factor user authentication in wireless sensor networks." Sensors 10, 2450–2459. https://doi.org/10.3390/s100302450

Khan, M.K., Kumari, S., 2013. An authentication scheme for secure access to healthcare services. J. Med. Syst. 37. https://doi.org/10.1007/s10916-013-9954-3

Koshy, P., Koshy, D., McDaniel, P., 2014. An analysis of anonymity in bitcoin using P2P network traffic, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, pp. 469–485. https://doi.org/10.1007/978-3-662-45472-5_30

Kshetri, N., 2018. 1 Blockchain's roles in meeting key supply chain management objectives. Int. J. Inf. Manage. 39, 80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Kuo, T., Kim, H., Ohno-machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Informatics Assoc. 24, 1211–1220. https://doi.org/10.1093/jamia/ocx068

Lamport, L., Shostak, R., Pease, M., 1982. The Byzantine Generals Problem. ACM Trans. Program. Lang. Syst. 4, 382–401.

Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B., 2010. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, in: Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). pp. 62–91. https://doi.org/10.1007/978-3-642-13190-5_4

Lewko, A., Waters, B., 2011. Decentralizing Attribute-Based Encryption, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp. 568–588.

Li, C., MahaDeVan, S., Ling, Y., Choze, S., Wang, L., 2017. Dynamic Bayesian network for aircraft wing health monitoring digital twin. AIAA J. 55, 930–941. https://doi.org/10.2514/1.J055201

Li, F., Xiong, P., 2013. Practical secure communication for integrating wireless sensor networks into the internet of things. IEEE Sens. J. 13, 3677–3684. https://doi.org/10.1109/JSEN.2013.2262271

Li, J., Au, M.H., Susilo, W., Xie, D., Ren, K., 2010. Attribute-based signature and its applications, in: Proceedings of the 5th International Symposium on Information, Computer and Communications Security, ASIACCS 2010. pp. 60–69. https://doi.org/10.1145/1755688.1755697

Li, J., Chen, X., Chow, S.S.M., Huang, Q., Wong, D.S., Liu, Z., 2018a. Multi-authority fine-grained access control with accountability and its application in cloud. J. Netw. Comput. Appl. 112, 89–96. https://doi.org/10.1016/j.jnca.2018.03.006

Li, J., Li, Y.K., Chen, X., Lee, P.P.C., Lou, W., 2015a. A Hybrid Cloud Approach for Secure Authorized Deduplication. IEEE Trans. Parallel Distrib. Syst. 26, 1206–1216. https://doi.org/10.1109/TPDS.2014.2318320

Li, J., Liu, Z., Chen, X., Xhafa, F., Tan, X., Wong, D.S., 2015b. L-EncDB: A lightweight framework for privacy-preserving data queries in cloud computing. Knowledge-Based Syst. 79, 18–26. https://doi.org/10.1016/j.knosys.2014.04.010

Li, J., Zhang, Y., Chen, X., Xiang, Y., 2018b. Secure attribute-based data sharing for resource-limited users in cloud computing. Comput. Secur. 72, 1–12. https://doi.org/10.1016/j.cose.2017.08.007

Li, Jin, Chen, X., Li, M., Li, Jingwei, Lee, P.P.C., Lou, W., 2014. Secure Deduplication with Efficient and Reliable Convergent Key Management. IEEE Trans. Parallel Distrib. Syst. 25, 1615–1625. https://doi.org/10.1109/tpds.2013.284

Li, J., Huang, X., Li, Jingwei, Chen, X., Xiang, Y., 2013. Securely Outsourcing Attribute-Based Encryption with Checkability. IEEE Trans. Parallel Distrib. Syst. 25, 2201–2210.

Li, Jin, Li, Jingwei, Chen, X., Jia, C., Lou, W., Member, S., 2015c. Identity-based Encryption with Outsourced Revocation in Cloud Computing. IEEE Trans. Comput. 64, 425–437. https://doi.org/10.1109/tc.2013.208

Li, L.H., Lin, I.C., Hwang, M.S., 2001. A remote password authentication scheme for multiserver architecture using neural networks. IEEE Trans. Neural Networks 12, 1498–1504.

https://doi.org/10.1109/72.963786

Li, M., Yu, S., Zheng, Y., Ren, K., Lou, W., 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Trans. Parallel Distrib. Syst. 24, 131–143. https://doi.org/10.1109/TPDS.2012.97

Li, S., Xu, L. Da, Zhao, S., 2018. 5G Internet of Things: A survey. J. Ind. Inf. Integr. 10, 1–9. https://doi.org/https://doi.org/10.1016/j.jii.2018.01.005

Liu, Y., He, D., Obaidat, M.S., Kumar, N., Khan, M.K., Raymond Choo, K.-K., 2020. Blockchain-based identity management systems: A review. J. Netw. Comput. Appl. 102731. https://doi.org/10.1016/j.jnca.2020.102731

Lumini, A., Nanni, L., 2007. An improved BioHashing for human authentication. Pattern Recognit. 40, 1057–1065. https://doi.org/10.1016/j.patcog.2006.05.030

Luu, L., Chu, D.H., Olickel, H., Saxena, P., Hobor, A., 2016. Making smart contracts smarter, in: Proceedings of the ACM Conference on Computer and Communications Security. pp. 254–269. https://doi.org/10.1145/2976749.2978309

McCain, K.W., 1990. Mapping authors in intellectual space: A technical overview. J. Am. Soc. Inf. Sci. 41, 433–443. https://doi.org/10.1002/(SICI)1097-4571(199009)41:6<433::AID-ASI11>3.0.CO;2-Q

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S., 2013. A fistful of Bitcoins: Characterizing payments among men with no names, in: Proceedings of the 2013 Conference on Internet Measurement Conference. ACM. pp. 127–140. https://doi.org/10.1145/2896384

Merkle, R.C., 1987. A Digital Signature Based on a Conventional Encryption Function, in: Pomerance, C. (Ed.), Lecture Notes in Computer Science 293. Springer, Berlin, Heidelberg, pp. 640–648. https://doi.org/https://doi.org/10.1007/3-540-48184-2_32

Miers, I., Garman, C., Green, M., Rubin, A.D., 2013. Zerocoin: Anonymous distributed e-cash from bitcoin, in: Proceedings - IEEE Symposium on Security and Privacy. pp. 397–411. https://doi.org/10.1109/SP.2013.34

Nakamoto, S., 2008. Bitcoin: A Peer-to Peer Electronic Cash System [WWW Document]. URL https://bitcoin.org/bitcoin.pdf (accessed 6.12.19).

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press.

Negri, E., Fumagalli, L., Macchi, M., 2017. A Review of the Roles of Digital Twin in CPS-based Production Systems. Procedia Manuf. 11, 939–948. https://doi.org/10.1016/j.promfg.2017.07.198

Nerur, S.P., Rasheed, A.A., Natarajan, V., 2008. The intellectual structure of the strategic management field: An author co-citation analysis. Strateg. Manag. J. 29, 319–336. https://doi.org/10.1002/smj.659

Oliveira, L.B., Aranha, D.F., Gouvêa, C.P.L., Scott, M., Câmara, D.F., López, J., Dahab, R., 2011. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. Comput. Commun. 34, 485–493. https://doi.org/10.1016/j.comcom.2010.05.013

Ostrovsky, R., Sahai, A., Waters, B., 2007. Attribute-based encryption with non-monotonic access structures, in: Proceedings of the ACM Conference on Computer and Communications Security. pp. 195–203. https://doi.org/10.1145/1315245.1315270

Pal, S., Hitchens, M., Varadharajan, V., 2019. Modeling identity for the internet of things: Survey, classification and trends. Proc. Int. Conf. Sens. Technol. ICST 2018-Decem, 45–51. https://doi.org/10.1109/ICSensT.2018.8603595

Qi, Q., Tao, F., 2018. Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison. IEEE Access 6, 3585–3593. https://doi.org/10.1109/ACCESS.2018.2793265

Reid, F., Harrigan, M., 2013. An analysis of anonymity in the bitcoin system. Secur. Priv. Soc. Networks 197–223. https://doi.org/10.1007/978-1-4614-4139-7_10

Rivest, R.L., Shamir, A., Adlemann, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 120–126. https://doi.org/10.1145/359340.359342

Roman, R., Lopez, J., 2009. Integrating wireless sensor networks and the internet: A security analysis. Internet Res. 19, 246–259. https://doi.org/10.1108/10662240910952373

Roman, R., Zhou, J., Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Comput. Networks 57, 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Ron, D., Shamir, A., 2014. Quantitative Analysis of the Full Bitcoin Transaction Graph, in: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-39884-1

Rosen, R., Von Wichert, G., Lo, G., Bettenhausen, K.D., 2015. About the importance of autonomy and digital twins for the future of manufacturing. IFAC-PapersOnLine 28, 567–572. https://doi.org/10.1016/j.ifacol.2015.06.141

Rouselakis, Y., Waters, B., 2013. Practical constructions and new proof methods for large universe attribute-based encryption, in: Proceedings of the ACM Conference on Computer and Communications Security. pp. 463–474. https://doi.org/10.1145/2508859.2516672

Sahai, A., Waters, B., 2005. Fuzzy Identity-Based Encryption, in: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer Berlin Heidelberg, pp. 457–473.

Sarma, A.C., Girão, J., 2009. Identities in the future internet of things. Wirel. Pers. Commun. 49, 353–363. https://doi.org/10.1007/s11277-009-9697-0

Schleich, B., Anwer, N., Mathieu, L., Wartzack, S., 2017. Shaping the digital twin for design and production engineering. CIRP Ann. - Manuf. Technol. 66, 141–144. https://doi.org/10.1016/j.cirp.2017.04.040

Schnorr, C.-P., 1991. Efficient signature generation by smart cards. J. Cryptol. 4, 161–174.

Schroeder, G.N., Steinmetz, C., Pereira, C.E., Espindola, D.B., 2016. Digital Twin Data Modeling with AutomationML and a Communication Methodology for Data Exchange. IFAC-PapersOnLine 49, 12–17. https://doi.org/10.1016/j.ifacol.2016.11.115

Shae, Z., Tsai, J.J.P., 2017. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine, in: International Conference on Distributed Computing Systems. IEEE, pp. 1972–1980. https://doi.org/10.1109/ICDCS.2017.61

Shamir, A., 1985. Identity-Based Cryptosystems and Signature Schemes. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 196 LNCS, 47–53. https://doi.org/10.1007/3-540-39568-7_5

Shen, J., Wang, C., Li, T., Chen, X., Huang, X., Zhan, Z.H., 2018a. Secure data uploading scheme for a smart home system. Inf. Sci. (Ny). 453, 186–197. https://doi.org/10.1016/j.ins.2018.04.048

Shen, J., Zhou, T., Chen, X., Li, J., Susilo, W., 2018b. Anonymous and Traceable Group Data Sharing in Cloud Computing. IEEE Trans. Inf. Forensics Secur. 13, 912–925. https://doi.org/10.1109/TIFS.2017.2774439

Shen, Jian, Gui, Z., Ji, S., Shen, Jun, Tan, H., Tang, Y., 2018c. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J. Netw. Comput. Appl. 106, 117–123. https://doi.org/10.1016/j.jnca.2018.01.003

Shim, K.A., 2014. S2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks. Ad Hoc Networks 19, 1–8. https://doi.org/10.1016/j.adhoc.2014.01.011

Shim, K.A., Lee, Y.R., Park, C.M., 2013. EIBAS: An efficient identity-based broadcast authentication scheme in wireless sensor networks. Ad Hoc Networks 11, 182–189. https://doi.org/10.1016/j.adhoc.2012.04.015

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., Gidlund, M., 2018. Industrial Internet of Things: Challenges, Opportunities, and Directions. IEEE Trans. Ind. Informatics 14, 4724–4734. https://doi.org/10.1109/TII.2018.2852491

Small, H.G., 1977. A Co-Citation Model of a Scientific Specialty: A Longitudinal Study of Collagen Research. Soc. Stud. Sci. 7, 139–166. https://doi.org/10.1177/030631277700700202

Small, H.G., 1973. Co-citation in the scientific literature: A new measure of the relationship between two documents. J. Am. Soc. Inf. Sci. 24, 265–269. https://doi.org/10.1002/asi.4630240406

Tao, F., Cheng, J., Qi, Q., Zhang, M., Zhang, H., Sui, F., 2018a. Digital twin-driven product design, manufacturing and service with big data. Int. J. Adv. Manuf. Technol. 94, 3563–3576. https://doi.org/10.1007/s00170-017-0233-1

Tao, F., Zhang, M., 2017. Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing. IEEE Access 5, 20418–20427. https://doi.org/10.1109/ACCESS.2017.2756069

Tao, F., Zhang, M., Liu, Y., Nee, A.Y.C., 2018b. Digital twin driven prognostics and health management for complex equipment. CIRP Ann. 67, 169–172. https://doi.org/10.1016/j.cirp.2018.04.055

Tschorsch, F., Scheuermann, B., 2016. Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Commun. Surv. Tutorials 18, 2084–2123.

https://doi.org/10.1109/COMST.2016.2535718

Tuegel, E.J., Ingraffea, A.R., Eason, T.G., Spottswood, S.M., 2011. Reengineering aircraft structural life prediction using a digital twin. Int. J. Aerosp. Eng. 2011. https://doi.org/10.1155/2011/154798

Turkanović, M., Brumen, B., Hölbl, M., 2014. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks 20, 96–112. https://doi.org/10.1016/j.adhoc.2014.03.009

Uhlemann, T.H.J., Lehmann, C., Steinhilper, R., 2017. The Digital Twin: Realizing the Cyber-Physical Production System for Industry 4.0. Procedia CIRP 61, 335–340. https://doi.org/10.1016/j.procir.2016.11.152

van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., Zarin, N., 2019. Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology 1–8.

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

Veletsianos, G., 2012. Higher education scholars' participation and practices on Twitter. J. Comput. Assist. Learn. 28, 336–349. https://doi.org/10.1111/j.1365-2729.2011.00449.x

Wang, D., He, D., Wang, P., Chu, C.H., 2015. Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment. IEEE Trans. Dependable Secur. Comput. 12, 428–442. https://doi.org/10.1109/TDSC.2014.2355850

Waters, B., 2011. Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization, in: International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, pp. 53–70. https://doi.org/10.1016/j.ins.2013.12.027

Wernke, M., Skvortsov, P., Dürr, F., Rothermel, K., 2014. A classification of location privacy attacks and approaches. Pers. Ubiquitous Comput. 18, 163–175. https://doi.org/10.1007/s00779-012-0633-z

Wollschlaeger, M., Sauter, T., Jasperneite, J., 2017. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. IEEE Ind. Electron. Mag. 11, 17–27. https://doi.org/10.1109/MIE.2017.2649104

Wörfel, P., 2019. Unravelling the intellectual discourse of implicit consumer cognition: A bibliometric review. J. Retail. Consum. Serv. 101960. https://doi.org/10.1016/j.jretconser.2019.101960

Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M., 2017. MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain. IEEE Access 5, 14757–14767. https://doi.org/10.1109/ACCESS.2017.2730843

Xiong, H., Qin, Z., 2015. Revocable and Scalable Certificateless Remote Authentication Protocol with Anonymity for Wireless Body Area Networks. IEEE Trans. Inf. Forensics Secur. 10, 1442–1455. https://doi.org/10.1109/TIFS.2015.2414399

Xu, J., Wei, L., Zhang, Y., Wang, A., Zhou, F., Gao, C. zhi, 2018. Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures. J. Netw. Comput. Appl. 107, 113–124. https://doi.org/10.1016/j.jnca.2018.01.014

Xue, K., Ma, C., Hong, P., Ding, R., 2013. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J. Netw. Comput. Appl. 36, 316–323. https://doi.org/10.1016/j.jnca.2012.05.010

Yu, H., Kaminsky, M., Gibbons, P.B., Flaxman, A.D., 2008. SybilGuard: Defending against sybil attacks via social networks. IEEE/ACM Trans. Netw. 16, 576–589. https://doi.org/10.1109/TNET.2008.923723

Yu, S., Wang, C., Ren, K., Lou, W., 2010. Achieving secure, scalable, and fine-grained data access control in cloud computing, in: Proceedings - IEEE INFOCOM. https://doi.org/10.1109/INFCOM.2010.5462174

Yue, X., Wang, H., Jin, D., Li, M., Jiang, W., 2016. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 40, 218. https://doi.org/10.1007/210916-016-0574-66

Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T., 2018. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput. Struct. Biotechnol. J. 16, 267–278. https://doi.org/10.1016/j.csbj.2018.07.004

Zhang, Y., Chen, X., Li, J., Wong, D.S., Li, H., You, I., 2016. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Inf. Sci. (Ny). 378, 42–61. https://doi.org/10.1016/j.ins.2016.04.015

Zhang, Y., Zheng, D., Deng, R.H., 2018. Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control. IEEE Internet Things J. 5, 2130–2145. https://doi.org/10.1109/JIOT.2018.2825289

Zheng, Y., 1999. Signcryption or How to Achieve Cost Signature & Encryption Cost Signature + Cost Encryption, in: Annual International Cryptology Conference. Springer, Berlin, Heidelberg.

Zupic, I., Čater, T., 2015. Bibliometric Methods in Management and Organization. Organ. Res. Methods 18, 429–472. https://doi.org/10.1177/1094428114562629

Zuschke, N., 2019. An analysis of process-tracing research on consumer decision-making. J. Bus. Res. 1–16. https://doi.org/10.1016/j.jbusres.2019.01.028

Declarations

Availability of data and materials

The datasets used and/or analyzed during the current study are available from the corresponding author on request.

Conflicts of interest

Not applicable.

Funding

The authors received funding through the project STEREO, which has been funded through the framework of the showcase programme Secure Digital Identities of the Bundesministerium für Wirtschaft und Energie (BMWi) under funding code 01MN200006E. The funding source was not involved in the study apart from the financial support.

Acknowledgements

Not applicable.

About the Blockchain Research Lab

The Blockchain Research Lab promotes independent science and research on blockchain technologies and the publication of the results in the form of scientific papers and contributions to conferences and other media. The BRL is a non-profit organization aiming, on the one hand, to further the general understanding of the blockchain technology and, on the other hand, to analyze the resulting challenges and opportunities as well as their socio-economic consequences.

www.blockchainresearchlab.org