A Visual Analysis of Research on Information Security Risk by Using CiteSpace

XIAOTONG LI AND **HUA LI**

[1] School of Economics and Management, Xidian University, Xi'an, China
[2] Shaanxi Soft Science Institute of Informatization and Digital Economy, Xidian University, Xi'an, China

Corresponding author: Hua Li (lihua@xidian.edu.cn)

ABSTRACT The security of information issue has become a global problem and has risen the concerns of both researchers and practitioners. When security incidents occur, there is a risk that national military secrets or confidential information of corporations will leak out and cause serious damages to the collective. This paper is aimed to explore the knowledge structure, development, and the future trend of information security area by providing a comprehensive review of the present information security risk (ISR) literature. The visualization analysis was conducted on journal literatures from the Web of Science, IEEE, ACM, and Scopus database, and the results were mapped into the I-model. According to 2748 articles, evaluation methods, e.g., frequency statistics, clustering coefficient, and centrality calculation, are employed to analyze all of the interrelated matrixes that are supported by CiteSpace. Some useful outcomes of a variety of objectives are shown under a significant level, such as author, country/territory, cluster, institute, as well as reference. A synthetical analysis has demonstrated the future research trend on ISR. As for researchers and practitioners, this paper suggests an analysis of integrated visualization in terms of the knowledge and innovation based on the area of ISR.

INDEX TERMS Visualization, information security risk, knowledge mapping, Web of Science, CiteSpace.

I. INTRODUCTION

As we are living in the information era, with the development of international Internet technology, challenges and opportunities coexist with globalization, it is vital to improve information security. Information protection has become an important issue for international businesses, e.g., the confidential information in terms of intellectual property and trading, and the mission-critical and safety-critical IT services destruction, as employed via the providers of service. Social networking and cloud computing technology trends show that the novel methods for the leakage of information has tremendous destruction to reputations and the advantage and incomes in such competition [1], [2]. A recent McKinsey research shows that by 2020 the economic losses could reach $20 trillion because of cyber-attacks [3]. The abuse of security is manifested in human factors, the vulnerability of system, the technical failure, as well as external events [4], [5]. Consequently, the security of information has become especially vital to the business survival and success to maintain the informational integrality, practicability, as well as the confidentiality.

The analysis of information security risks requires critical task asset awareness, the key task asset losses impact, as well as the potential threats which could undermine the capability of a mission [6]. The threats of information security come in a number of different forms. Several common threats are software attacks, intellectual property rights violations, confidential information disclosure, and the extortion of information. Hence, some information security solutions have been developed, but they are primarily focused on the analysis of the IT system vulnerabilities and threats, and how to lower the risk to the approved standard [7]. It is suggested that enterprises adopt the method of risk management to manage the security of information, i.e., information security risk management (ISRM) including identification, review, management and assessment of risk, among which information risk assessment is of the core activity and is the critical process. Assessment of risk starts with identifying risks, then prioritizing them, determining the suitable techniques, and finally examining the states [8]. Therefore, many different types of risk assessment standards and methods can be referenced, including both quantitative and qualitative methods [9], [10], many of

the current studies combine these two approaches for risk assessment [11]–[13]. Each of them is performed to meet specific needs, so there are different constructions, purposes, steps, as well as application standards. Three distinct phases are defined in the assessment of information risk: background establishment, risk identification and risk analysis [14]. The shared goal is to invent risk handling projects and demonstrate the cost of control options, the pursuit of progress, maintenance of management as well as installation.

In recent years, a large number of new techniques like CiteSpace have enhanced the visualization of knowledge to a great extent. Visual clarity and the ability have evolved to interpret new CiteSpace software [15]. In early 2004, software CiteSpace was created by Chen [16], which visualizes and analyzes the trends and patterns in scientific literature as a freely available Java application. Recently, this software has been updated with new versions to CiteSpace II or CiteSpace III. Similarly, it can be analogous to cameras that capture snapshots of certain areas based on time series and links to deduce trends and changes in the area. The software is dedicated to finding critical points, especially critical points, in the development of this particular area [15]. CiteSpace conducted a structured and time-critical analysis of the various networks produced by scientific publications, including the author's Common Citation Network, the Reference Citation Network, and the Cluster Citation Timeline. It also supports hybrid node-type networks such as countries, agencies, authors, and some hybrid link types, such as co-occurrences, co-referencing, and referencing links. The main input source for this software is ScienceNet including complete documentation and reference material. Users can evaluate the knowledge base, hot spots, key points, as well as articles of a stack of articles. Recently, many researchers have used this software to examine their direction: visualizing mass extinctions and terrorism [15], visualization of research data and knowledge engineering [17], visualization of electronic publishing [18], visualization of pervasive computing domain [19], visualization based on subject calculations [20], visualization of oil and flax studies [21], visualization of terahertz technology [22], visualization of ecological values/assets [23], as well as visual analysis of energy analysis [24].

The purpose of this paper is to provide a visual overview of the related articles based on mapping knowledge. The key articles identified are the ISRs, and the metrics for scientific metrology and visual identity analysis are used, including the results of key terms such as countries, agencies, highly cited authors, leading articles and journals, and major research hot spots, etc. These results are mapped into the I-model and panoramic information in this filed is revealed in this way. The ultimate aim of this study is applying ISR acting as a framework for visual quantitative research employing Citespace.

II. METHODOLOGY

This study uses CiteSpace citation software to obtain visual information of "Information security risks" or "information

security risk" or "IT security risk" is searched on the web of Science, IEEE, ACM and Scopus databases and recent ten years are choose from the databases, all data is available online from January 2007 to May 2018. Reviews, articles, program files as well as book reviews have already been recorded. In the period from2007 to 2018, there were 2748 journal articles that were downloaded and recorded from this database. The search details are summarized in Table 1 [25].

TABLE 1. Summary of searching details.

Source	Web of Science; IEEE; ACM; Scopus
Citation indexes	SCI-EXPANDED; SSCI; CPCI-S; CPCI-SSH
Years	January, 2007-May, 2018
Searching terms	"Information security risks" or "information security risk" or "IT security risk"
Sample size	2748

All the relational matrices were analyzed employing the methods of frequency statistics, center calculation as well as clustering coefficient. After that, several typical matrix mappings were chosen to display.

III. RESULTS AND ANALYSES

A full set of records for 2748 journal articles were retrieved and downloaded in May 2018. The number of publications for each year is displayed in Figure 1. In general, the number of publications shows a rising trend and has reached a summit at approximately 400 publications in 2017.There were two obvious increases after 2008 and 2016. The first jump occurs after the "Snowstorm incident", and the second jump may due to some phishing attacks, identity theft, eavesdropping, and other security breaches, such as the data leakage in Yahoo and MySpace, etc.

A. EQUATIONS CO-AUTHOR'S COUNTRY/REGION AND AGENCY ANALYSIS

First, some basic parameter settings are listed: pruning, time slicing, and linking. Study time was recorded from 2007 to 2018. Minimum Spanning Tree (MST) as well as Pathfinder are two common algorithms of network pruning as supported by CiteSpace. Due to its simple operation, we focus on the MST. In the present study, the cosine function is used to handle the strength between cluster links and nodes, with the range type set as "within slices". In the following sections, a number of options have been chosen to analyze the parameters based on the centrality, and to look at the frequencies and networks by a variety of ways.

As shown in Figure 2, from 2007 to 2018, 75 nodes and 95 links in the partner countries formed a network. Another point to note here is that the different time zones have different colours; the central country/ territory is described by the circle size. The lines between the two nodes represent
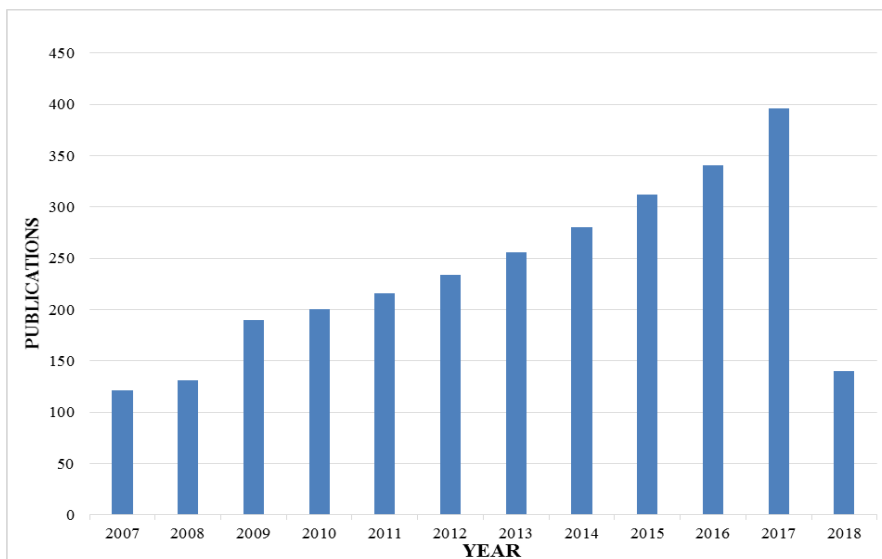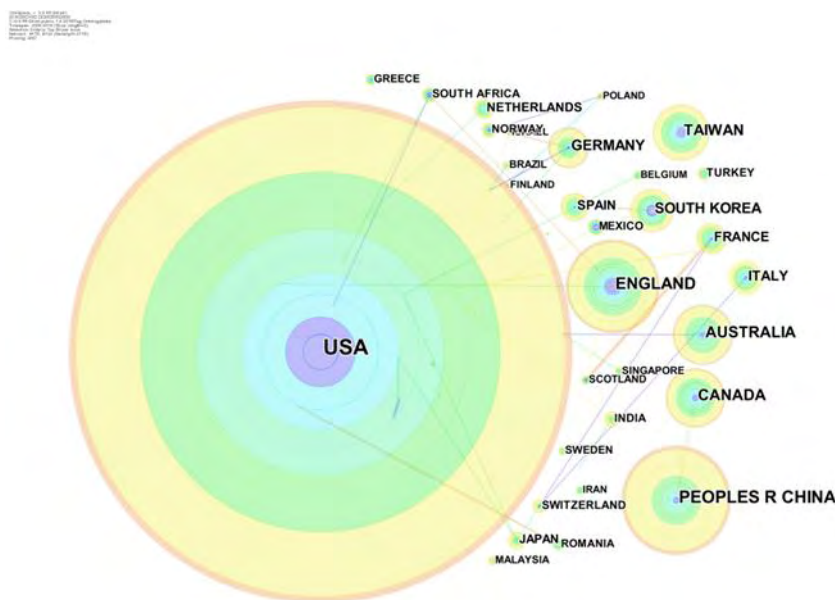
FIGURE 1. Number of publications.

FIGURE 2. Joint mapping of productive countries/ territories.

the collaboration links, the intensity of which is proportional to the thickness of the line. Ten countries in the region dominate. The total publication of Table 2 shows that the United States has published 1221 papers, making the most significant contribution. Since the United States is the first country in the world to start information technology and network technology, it is also a country with more systematic laws and regulations on information security. In addition, due to the ''9.11'' incident and the ''Snowstorm incident'' (PRISM), the strategic status of information security has been escalating, leading many researchers to start research in the field of information security. This is followed by 335 articles

of China. China is a developing country with a large population base and many Internet users. At present, China has established some think-tank information security research, so this reality requirement has played a facilitating role in the academia. Britain is the third contributor to 311 papers. The number of publications in Australia was 171, ranking fourth, followed by Canada, with 162 papers published. Some European nations have also made great contributions, i.e., Germany (91), Italy (76) and France (66), followed by Japan, Mexico, Norway, India and other countries.

Figure 3 shows the main distribution of production facilities. It should be noted that the analysis of all publications
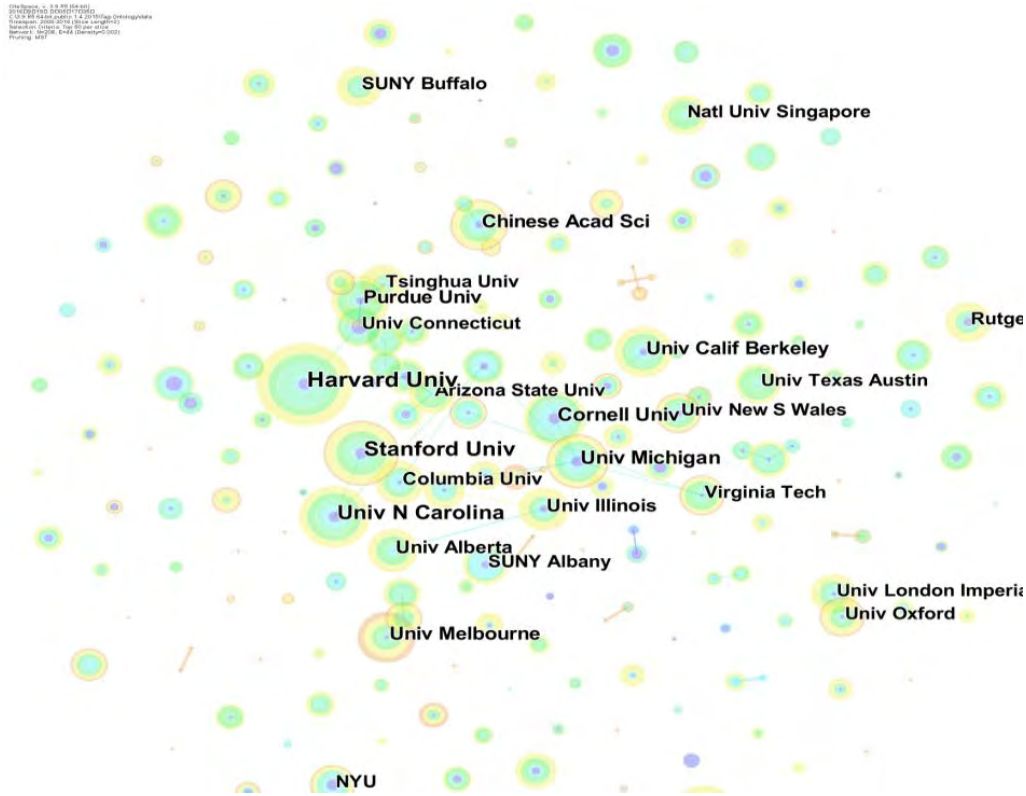
FIGURE 3. Production agencies joint mapping.

TABLE 2. Top 10 most productive countries/territories.

Total publication	Countries/ territories	Total publication	Countries/ territories
1221	USA	139	Taiwan
335	People R China	91	Germany
311	England	81	South Korea
171	Australia	76	Italy
162	Canada	66	France

is based on 133 research institutes. Evidently, the major research institutes are mainly from the United States, China, the United Kingdom, Australia as well as Canada. In the United States, Harvard University, Stanford University, University of Michigan, University of North Carolina, Purdue University, Cornell University, Berkeley, etc., are the major research institutes. In the following China, the most productive counterparts primarily include Tsinghua University, Chinese academic sciences, University of Hong Kong, Peking University, Chinese University of Hong Kong, etc.; in the UK, they are Dartmouth College, the Imperial College London, Oxford, etc.; in Australia, productive research institutions includes Deakin University, the University of Melbourne, University of New South Wales as well as Australian National University. Table 3 shows the top ten major institutions. There are 23 published articles in Harvard, ranking first, and the second is Stanford University with 18 papers published. Obviously, most of the productive research institutes come

TABLE 3. The top 10 most productive institutes.

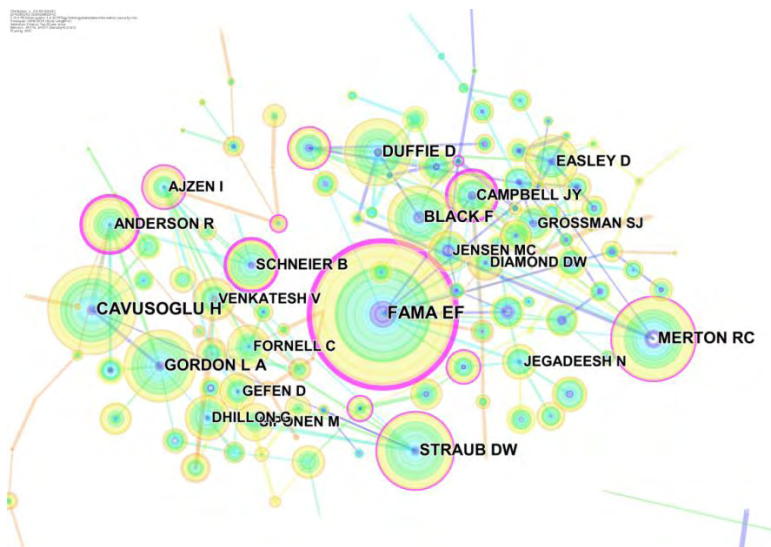| Total publication	Institute	Total publication	Institute
23	Harvard University	14	Purdue University
18	Stanford University	14	National Taiwan University
17	University of North Carolina	14	University of California Berkeley
15	Cornell University	14	University of Melbourne
15	University of Michigan	14	Chinese Academic Science

FIGURE 4. Joint mapping of productive authors.

TABLE 4. The top 20 most productive authors.

Total publication	Author	Total publication	Author
147	Fama EF	55	Campbell JY
96	Cavusoglu H	51	Dhillon G
85	Merton RC	50	Ajzen I
82	Straub DW	49	Fornell C
80	Gordon L A	48	Amihud Y
75	Duffie D	48	Venkatesh V
72	Black F	47	Grossman SJ
63	Easley D	46	Jensen MC
61	Anderson R	45	World Health Organization
58	Schneier B	45	Siponen M

from the United States, China, and the United Kingdom. A number of other institutes are expected to continue contributing to the ISR area, such as University of Alberta and Korea University. As a result, it is evident that major research institutes and universities have made great contributions to the field of ISR, and some companies are also striving to achieve that, e.g., Cyber Pack Ventures with one published paper associated with ISR.

B. ANALYSIS OF CO-REFERENCE CREATORS, CO-REFERENCE REFERENCES AND JOURNALS

In Figure 4, the joined mapping of productive creators is shown in the field of ISR, with 176 authors as well as 248 co-reference joins described. The quantity of information security published papers is correspondingly proportional to the node estimated size. The line between two nodes is made on behalf of a co-reference connect, and the quality

of co-reference is relative to the line thickness. The distance between two circles is conversely corresponding to the collaboration between each author, demonstrating that shorter distance indicates more participation. In Figure 4, the green color equals to middle years; the shade of blue equivalents to the earlier papers; the yellow and red states the late publications. It could be seen from Table 4 that Fama is the top profitable author directing the best agreeable positions with the biggest reference circle. Different authors with top reference include Merton (85), Straub (82), Gordo (80), Duffie (75), Black (72), etc.

The highly-referred ISR articles are acquired via co-reference examination. Figure 5 demonstrates a system of article co-reference is left the referring to writers citing behaviors. 264 co-reference joins and 184 papers are summarized. In Figure 5, each node is made representing one referred article. Likewise, the reference number of is relative
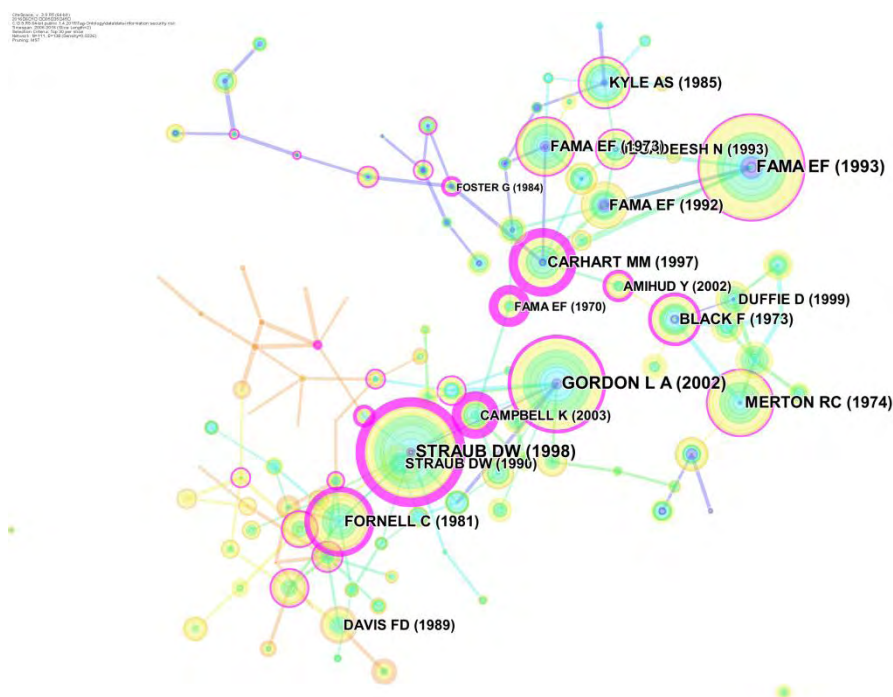
FIGURE 5. Combined mapping of co-citation references.

to the ring thickness. 2 years cuts are shown from 2007 to 2018. The shade of blue connections is made representing the earliest years; the shades of green and yellow are made representing mid-range years; the shade of orange is made representing late years. In Figure 5, the highly-cited articles on the premise of circle's size are papers of Fama', Gordon L, Straub, Merton, and Fornell et cetera. Fama's work was found in blue and orange from inside to outside, implying that his work was referred to since ever published to now. It appears that in recent years Straub's paper has been referred to, as a result of the shades of red and orange. Practically after the time of 2007 the paper by Straub was referred to.

According to the quotation frequency of Table 5, the top 20 most frequently quoted articles are summarized. It can been observed that Fama and French's [26] paper was quoted 68 times, winning the first place and suggesting it to be the most important article. Five common risk factors are identified for returns on the stocks and bonds and thus explains the average return on the bonds and the equities. In Table. 5, two papers have been cited 41 for times, 36 times respectively. This paper first tests the relationship between the NYSE risk and average return on the New York Stock Exchange. The theoretical basis of the test is the "two-parameter" portfolio model and the market equilibrium model based on the two-parameter portfolio model. There are two easily measurable variables described in this paper, i.e., size and book value of the market value of the stock, which is combined with the average stock returns of the representative variables acquired with the market beta, size, leverage, as well as book value to market capitalization, and earnings- price ratio. Gordon and Loeb's [27] article was quoted 61 times and

occupied the second place. An economic model is proposed to determine the optimal amount of investment to protect certain information. Straub and Welke's [28] paper was cited 60 times, ranking the third. This paper examines systemic risk management decisions by establishing a model of safety planning. He suggests that managers are often lacking the full control over which knowledge is available to achieve the most usable controls. They promoted the well-educated sense of employee safety awareness and analytic countermeasures to solve such problem by applying a model of security risk planning. Another Straub, Jr., [29] paper is cited 31 times. On the basis of the criminal theory of general deterrence, this study examines whether investment management decisions can effectively control the abuse of computer. Therefore, the information technology trend which is responsible for the security of information has been changed, and management is considered as the main reason for information security. In the management of information security, various management practices have been developed. A number of Merton's [30] papers are cited 46 times and ranked the fourth, developing a way to price corporate debt on the basis of sound economic analysis that can be used to price almost any type of financial instrument. Fornell and Larcker's [31] thesis and Carhart's [32] ranking the sixth and the seventh with 41 and 36 citations, respectively. Fornell promoted and employed a test system on the basis of the shared variance metric of structural models, measurement models as well as overall models to overcome the problems of current test methods. Cho's [33] thesis, Black and Scholes' [34] dissertation, Davis's [35] dissertation, Jegadeesh and Titman [36] dissertation, Duffie and Singleton's [37] articles are also

TABLE 5. Top 20 highly cited papers.

Cited frequency	Cited reference	Source	Volume	Page
68	Fama EF,1993	J FINANC ECON	V33	P3
61	Gordon L A,2002	ACM TISSEC	V5	P438
60	Straub DW,1998	MIS QUART	V22	P441
46	Merton RC,1974	J FINANC	V29	P449
41	Fama EF,1973	J POLIT ECON	V81	P607
41	Fornell C,1981	J MARKETING RES	V18	P39
36	Carhart MM,1997	J FINANC	V52	P57
36	Fama EF,1992	J FINANC	V47	P427
36	Kyle AS,1985	ECONOMETRICA	V53	P1315
34	Black F,1973	J POLIT ECON	V81	P637
31	Straub DW,1990	INFORM SYST RES	V1	P255
29	Davis FD,1989	MIS QUART	V13	P319
29	Jegadeesh N,1993	J FINANC	V48	P65
29	Duffie D,1999	REV FINANC STUD	V12	P687
28	Venkatesh V,2003	MIS QUART	V27	P425
28	Newey WK,1987	ECONAMETRICA	V55	P703
28	Jarrow RA,1995	J FINANC	V50	P53
28	Cavusoglu H,2004	INT J ELECTRON COMM	V9	P69
27	Jensen MC,1976	J FINANC ECON	V3	P305
26	Black F,1976	J FINANC	V31	P351

important in the area of ISR. It can be seen that an increasing number of researchers have realized that security failure is caused at least as often by bad economic incentives as by incompetent security technologies. Thus, many researchers have taken economic incentives into consideration to investigate how to manage information security effectively and economically. As a result, a new discipline, the information security economics emerged and became a thriving and fast-moving discipline.

The journal co-citation analysis could help us to discover the contributions of this journal and find suitable journals for submitting articles, so we list the top 10 highly cited journals in Table 6. It is easily to find out that "Computers & Security", "Information Systems Research" are important in the area of ISR, the other journals with high cited frequency such as "Decision Support Systems", "Journal of Financial Economics", "Computers in Human Behavior", "Journal of Banking & Finance", "MIS Quarterly", "Risk Analysis", "IEEE Access" and "Journal of Management Information Systems" are also play a crucial role in this area.

C. CO-CITATION GROUP ANALYSIS
Given that the highly cite articles of their co-citations are analyzed, they reflect the evolutionary process in a partic-

ular scientific activity. In this article, the tf $*$ idf weighting algorithm is chosen to reveal each co-citation cluster. In Figure 6, 10 co-citation clusters are presented with their keywords in a timeline view. As can be seen, from 1965 to 2014, the entire timeline is divided into five years. Similarly, different colors are on behalf of different years, from early years to recent years, in blue, green, yellow, and finally red colors, respectively. Table 7 summarizes the cluster IDs, sizes, sketches, average years, and labels for the articles on the ISR. Size indicates the number of articles contained in a given cluster. Cluster ID# 0is the largest cluster with the tag "Overreaction", it has 27 members and is one of the areas of greatest interest in the area. The most typical cited article is "Common Risk Factors for Stock and Bond Yields" (Fama, 1993). The second one is Cluster ID # 1 with the tag "Privacy" has 26 members. The third one is Cluster # 2 with "Organization" has 20 members and one of the typical citers is Albrechtsen (2007). This is followed by "Credit Expansion" (# 3) and "Principles" (# 4), they have 19 members and 18 members respectively. Cluster ID # 5 and cluster ID # 6 contain 14 members and 12 members, respectively labeled "Security" and "Securitization". Cluster ID # 7 has 11 members, focusing on "liquidity" where Kyle (1985) is prominent. Cluster ID # 8 and Cluster ID # 9 consist of

TABLE 6. Top 10 highly cited journals.

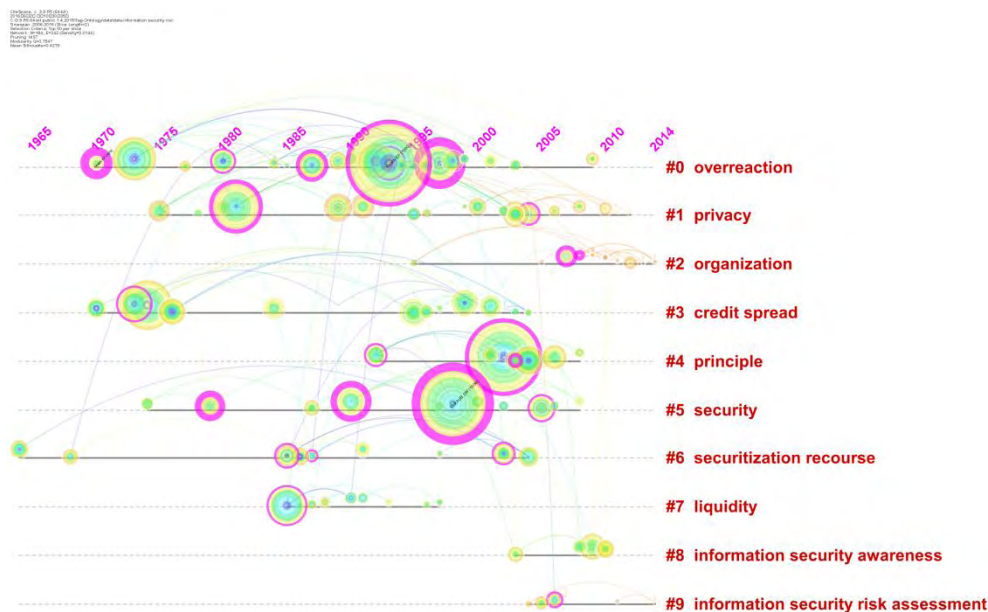| Journal	Frequency	Editor in chief	Scope
Computers & Security	69	Eugene H. Spafford	The International Source of Innovation for the Information Security and IT Audit Professional.
Information Systems Research	35	Alok Gupta	The journal covers a wide variety of phenomena and topics related to the design, management, use, valuation, and impact of information technologies at different levels of analysis.
Decision Support Systems	28	James R. Marsden	The journal is about theoretical and technical issues in the support of enhanced decision making. The areas addressed may include foundations, functionality, interfaces, implementation, impacts, and evaluation of decision support systems.
Journal of Financial Economics	26	G. William Schwert	This journal is a peer-reviewed academic journal covering the theory of financial economics. Together with the Journal of Finance and the Review of Financial Studies, it is considered to be among the three most prestigious finance journals in the world.
Computers in Human Behavior	24	Matthieu Guitton	This Journal is a scholarly journal dedicated to examining the use of computers from a psychological perspective.
Journal of Banking & Finance	24	Carol Alexander, Geert Bekaert	The journal publishes theoretical and empirical research papers spanning all the major research fields in finance and banking.
MIS Quarterly	23	Arun Rai	The journal is interested in the IS field, the management of IT resources, and the use, impact, and economics of IT.
Risk Analysis	23	L. Anthony Cox, Jr.	The topics of this journal are, human health and safety risks, microbial risks, engineering, mathematical modelling, risk characterization, risk communication, risk management and decision-making, risk perception, acceptability, and ethics, raws and regulatory policy, Ecological risks.
IEEE Access	21	Michael Pecht	The scope of this journal comprises all of IEEE's fields of interest, emphasizing applications-oriented and interdisciplinary articles.
Journal of Management Information Systems	19	Vladimir Zwass	This journal serves those investigating new modes of information delivery and the changing landscape of information policy making, as well as practitioners and executives managing the information resource.

Information aspect	Technology aspect	People aspect	Society aspect
Information assets Asset identification Knowledge-sharing platform Content security threats	Information technology Cloud computing Access control Quantum communication technology	Decision makers Awareness and training Major concern	Information disclosure effects

Behavior and Attitude
Decision making, Information security measures, Information Security investment(IT configuration, insurance, outsourcing), Knowledge sharing, Corresponding trading mechanism, Risk hedging mechanism, Risk profile, Policy

Theories in information security
AHP, PRA, Game theory, Grey theory, Fuzzy theory, FMEA, Decision-making process, Support Vector Machine, D-S theory, Protection motivation theory
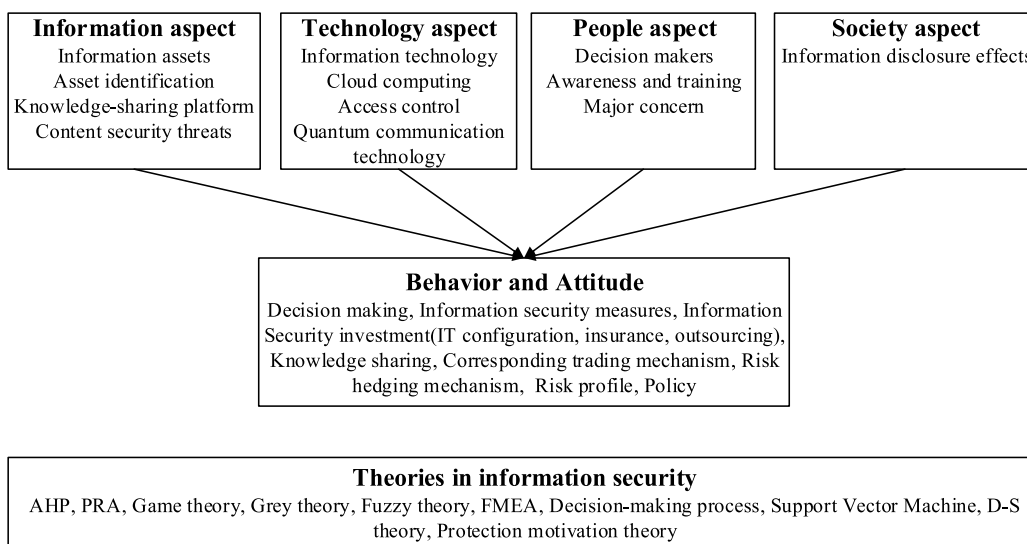
FIGURE 7. The integrated framework of information security risk researches.

10 members and 6 members, emphasizing "awareness of information security" and "risk assessment of information security".

The time distribution of co-citation clusters is isolated on the premise of the mean year in the period ranging from 1989 to 2009. In 1989, the earliest cluster is "asset securitization" or "securitization recourse" (#6) and it reveals that the issue of risk was seen from recourse of securitization. In Table 8, the clusters ID, mean year of this article, as well as marks are accounted. In Table 8, the significant time of the clusters are introduced to 1989– 1993 (4), 2004– 2009 (3), and 1994– 1998 (2). In a word, the trend of study in the area of ISR

from the cluster strategy have transformed from securitization of asset to data administration (risk control, identification of risk, knowledge sharing, analysis of risk, and assessment of risk).

D. ANALYSIS ON THE FACTORS FROM ABSTRACTS
We analyzed the key terms from abstracts and put them into the information model (I-model), which was developed by Zhang and Benjamin [38] and is, one of the most significant frameworks to study information security problems. There are four fundamental components were explained: information, technology, people, and society based on information

TABLE 7. The common citation clusters for ISR.

Cluster ID	Size	Silhouette	Mean(Year)	Label (tf*idf)
#0	27	0.751	1991	(12.54) overreaction; (12.54) Chinese stock market; (12.54) information diffusion; (11.11) arbitrage pricing theory model; (11.11) Bayesian variable selection
#1	26	0.868	1997	(13.61) privacy; (11.11) reducing online privacy risk; (11.11) corporate credibility; (11.11) e-service adoption; (10.98) influence
#2	20	0.886	2009	(15.01) organization; (14.47) information security knowledge sharing; (10.46) knowledge sharing; (10.16) personal information security behavior; (8.94) healthcare information protection intention
#3	19	0.957	1991	(13.61) credit spread; (13.61) stationary leverage ratio; (13.61) jump risk; (13.61) extended black-cox model; (13.61) default risk modeling
#4	18	0.886	2002	(9.2) principle; (8.94) security investment; (8.94) network vulnerability; (8.94) supply chain integration; (8.94) networked supply chain
#5	14	0.789	1995	(8.14) security; (7.26) information security; (7.21) assessment instrument; (7.21) information security culture; (7.21) case study
#6	12	0.747	1989	(8.94) securitization recourse; (8.94) asset securitization; (8.94) information uncertainty; (8.41) capital; (7.21) equity beta
#7	11	0.856	1990	(7.4) liquidity; (7.21) treasury bill; (7.21) trading activity; (7.21) market quality; (7.21) market-making cost
#8	10	0.844	2008	(7.17) information security awareness; (7.17) rationality-based belief; (6.92) security; (6.48) empirical study; (6.48) information security policy compliance
#9	6	0.961	2007	(7.21) information security risk assessment; (7.17) security risk; (6.16) security; (5.97) security risk analysis; (5.49) information security

TABLE 8. Article cluster ID, label and average year.

Mean year(range)	No. cluster	Cluster ID and labels
1989-1993	4	Securitization recourse(#6,1989); Liquidity(#7,1990); Overreaction(#0,1991); Credit spread(#3,1991)
1994-1998	2	Assessment instrument(#5,1995); Reducing online privacy risk(#1,1997)
1999-2003	1	Security investment(#4,2002)
2004-2009	3	Information security risk assessment(#9,2007); Information security awareness(#8,2008); Information security knowledge sharing(#2,2009)

security's properties and disciplines. Information are about library science and information science, technology mainly includes computer science and engineering, people derives from psychologies, sociologists, and cultural anthropologists, while society covers a number of aspects in many social sciences.

TABLE 9. The key terms of abstracts.

Independent variable	Dependent variable	Theory
Information assets	Decision-making	Game theory
Decision makers	Information security measures	Grey theory
Information technology	Risk assessment method	fuzzy theory
Assets identification	Information security investment	FMEA
Content security threats	Economic incentive	Decision-making process
Major concern	IT configuration	support vector machine
Awareness and training	Information security outsourcing	D-S theory
Security breaches	Information security insurance	AHP
Cloud computing	Knowledge sharing	PRA
Access control	Corresponding trading mechanism	Protection motivation theory
Knowledge-sharing platform	Risk hedging mechanism	
Maintenance	Risk profile	
Integrity	Security policy	
Identification and authentications	Quantum communication technology	

TABLE 10. Main research topics by year.

Year	Keyword	Centrality	Frequency	Year	Keyword	Centrality	Frequency
2007	Information security	0.38	825	2008	Framework	0.1	65
2007	Systems	0.18	167	2008	Trust	0.05	62
2007	Model	0.18	156	2008	Networks	0.06	54
2007	Management	0.07	143	2008	Protection motivation theory	0.02	49
2007	Cryptography	0.04	94	2008	Image encryption	0.06	45
2007	Scheme	0.22	76	2009	Perspective	0.05	54
2007	Risk	0.09	71	2009	Behavior	0.07	48
2007	Algorithm	0.11	69	2010	Privacy	0.1	91
2007	Authentication	0.07	68	2010	Organizations	0.04	53
2007	Decision-making	0.03	43	2013	Deterrence	0.01	42
2007	Intrusion detection	0.01	42	2013	Steganography	0.02	41
2007	Information security management	0.01	40	2014	Fear appeals	0.01	47
2008	Technology	0.09	67	2015	Knowledge sharing	0.01	42

We analyze the key terms of all abstracts in order to identify and summarize the factors and theories used in previous literature. As shown in Figure 7, a comprehensive integrated framework of information security risk researches has been presented. In Table 9, we screened key terms in all data abstract to reveal the elements with their frequency in the abstract, and then separated factors as independent variable, and dependent variable; some dependent variables may consist of intermediate variables. The independent variable is the variable that the decision maker actively manipulates, controls and influences the result. The dependent variable is the variable changed by the change of independent variable, and the dependent variable is logically behind the independent variable. Intermediate variable is a variable that cannot be observed and controlled, and its influence can only be inferred from the relationship between independent variable

FIGURE 8. Popular research topics.

TABLE 11. Top 40 keywords with strongest citation bursts.

Keywords	Strength	Begin	End	Keywords	Strength	Begin	End
Data security	4.87	2007	2008	Fractional fourier domain	3.21	2012	2013
Information system	3.74	2007	2008	Policy	3.04	2012	2013
Digital holography	3.28	2007	2011	Fractional fourier transform	4.04	2013	2014
Transform	3.04	2007	2008	Service	3.79	2013	2015
Ethics	3.55	2008	2009	Social engineering	2.60	2013	2016
Investment	3.34	2008	2012	Deterrence	5.83	2014	2015
Risk analysis	3.16	2008	2010	Classification	3.34	2014	2015
Simulation	3.16	2008	2010	Design	2.77	2014	2015
Incentive	2.66	2008	2009	Protection motivation theory	6.88	2015	2018
Implementation	2.94	2009	2012	Intention	6.43	2015	2017
Acceptance	3.62	2010	2014	User	4.64	2015	2017
Key management	2.74	2010	2011	Quality	4.60	2015	2016
Ad hoc network	2.74	2010	2011	Behavior	4.11	2015	2016
Risk management	4.67	2011	2014	Communication	3.43	2015	2016
Security policy	3.19	2011	2013	Protection motivation	3.37	2015	2018
Retrieval	2.74	2011	2013	Fear appeal	5.41	2016	2018
Standard	2.70	2011	2012	Knowledge sharing	4.76	2016	2018
Market value	2.70	2011	2012	Information security policy	4.51	2016	2018
Cloud computing	4.12	2012	2015	Risk profile	3.76	2016	2018
Economic incentive	3.81	2012	2013	Quantum communication technology	3.16	2016	2018

and dependent variable. Intermediate variables are mediating variables between cause and effect. Table 9 summarizes the relationship among research factors and commonly used theories in the research of information security to act as the guidance for future researches. We match the independent variables in table 9 to the I-model, it can be seen

that the threats to information security come mainly from the following four aspects, firstly, insufficient investment in the information security infrastructure; the lack of effective maintenance and maintenance systems for information security infrastructure; the lack of synchronization of design and construction. Secondly, basic information network and important information system security protection capability is not strong, and the level of information security from the perspective of technology requires improvement. Thirdly, deliberate attacks on hardware systems and natural disasters are the most danger ones. In this way, people factors, as the greatest threat to information security, are the most complex and active ones, which cannot be prevented via static methods, laws, or regulations. At last, disclosure of information may lead to both positive and negative effects. For instance, a firm may reveal that it has effectively taken careful steps to moderate the effect of negative occasions, for example, correspondence failures, attacks by the hackers, and so on. Due to the advent of the information security economics, this discipline has taken various economic and social factors into consideration, applied the theory of economics and management, resolved the conflict of interest of all information security stakeholders, and finally provided reasonable management implications of information security.

IV. POPULAR ISR RESEARCH TOPICS AND TRENDS

Co-occurring network analyses were performed using keywords such as ''node type''. Figure 8 shows the popular research topics in the ISR research arears include information security, systems, model, management, cryptography, privacy, scheme, risk, algorithm, authentication, decision-making and intrusion detection. Topics with high centrality include information security, scheme, systems, model, algorithm and privacy. Table 10 shows the main research topics by year. In order to show popular topics in different years and the evolutions among research topics clearly, we screened the keywords and selected them that appeared more than 40 times, and then checked whether these keywords showed centrality.

Table 11 shows the keywords with strongest citation bursts. Some of them show the first time the research topic appeared and its duration, such as main research topics coming out in 2007 included data security, information system, digital holography and transform, while topics in 2013 were fractional fourier transform, service and social engineering. Also, some research topics were identified as new trends in ISR research. There are some of the research topics still continue into 2018, such as protection motivation theory, protection motivation, fear appeal, knowledge sharing, information security policy, risk profile and quantum communication technology.

V. CONCLUSION

This paper exhibited a visual and scientometrics review of ISR in detail covering every related article from Scopus database and Web of Science from 2007 to 2018. Information

mapping and I-model are employed to explore this field. Some useful outcomes are shown with statistical information of various items (e.g., cluster, reference, country/territories, author, institute, and key terms).

The United States the first country in the world to start the information technology and network technology and also the country with more systematic information security laws and regulations. This is followed by China with a large population base and many netizens. China has established some think-tanks of information security research at present, so the reality demands play a promoting role in the academia. Several European nations also make a critical commitment, including Germany, France, and Italy. Additionally, huge establishments are chiefly from America, China, Australia, the United Kingdom, and Canada. In America, the primary research establishments incorporate Harvard University, Cornell University, Stanford University, etc.

By analyzing the highly cited papers and the contents of the I-model, some future research directions can be suggested. Firstly, according to the key terms of abstracts, like ''Information security investment'', ''Economic incentive'' and ''IT configuration'', it can be seen that an increasing number of researchers have realized that security failure is caused at least as often by bad economic incentives as by bad security technologies. Thus, many researchers have taken economic incentives into consideration to investigate how to manage information security effectively and economically. Secondly, there are some of the research topics still continue into 2018, such as protection motivation theory, protection motivation, fear appeal, knowledge sharing, information security policy, risk profile and quantum communication technology. Especially, ''Quantum communication'' is a new area of interdisciplinary science that has developed in the last twenty years, combining quantum theory with information theory. In recent years, this subject has steadily moved from theory to viable advancement. The data transmission of high proficiency and security is getting increasingly consideration. In light of the fundamental standards of quantum mechanics, it could turn into an exploration hotspot in quantum material science and data science universally. Thirdly, traditional decision-theory-based evaluation methods like ''AHP'' or ''PRA'' are unable to capture the strategic interaction. According to the I-model of theory in information security, ''Game theory'' is appropriate for modeling such strategic interactions. Besides, ''Information security outsourcing'' and ''Information security insurance'' are effective ways to improve the level of information security. Therefore, we suggest that researchers may find new insight into the contract theory to study the problems as well.

Disregarding utilizing a panoramic way to gather and sort relevant literature, there are still some constraints as to explore the terms and identified papers. First, we just utilized English terms to examine, so the distributions in different languages were excluded for this study. Second, a progression of predefined terms is utilized which may make

some articles remaining unspotted. In the process of literature investigation, a replaceable pursuit process with terms gathered ought to be discovered with more significant literature. Thirdly, this paper could enhance our comprehension if some empirical tests employing quantitative studies and qualitative case studies are utilized. It additionally suggests researchers should hold an administration viewpoint and concentrate on security related issues in risk hedging mechanism, information security investment as well as quantum communication technology.

All summaries of this study depended on literature from Scopus database as well as Web of Science, and the target was to suggest a strategy for taking out the valuable data from extensive literature. As a result of the distinctions in quality and quantity of test samples, a few conclusions may be one-sided. Hence, we will keep on promoting this study later on.

REFERENCES

[1] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.

[2] B. Hauer, "Data and information leakage prevention within the scope of information security," *IEEE Access*, vol. 3, pp. 2554–2565, 2015.

[3] D. Chinn, J. Kaplan, and A. Weinberg, *Risk and Responsibility in a Hyperconnected World: Implications for Enterprises*. New York City, NY, USA: McKinsey & Company, 2014, pp. 1–40.

[4] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *Int. J. Inf. Manage.*, vol. 28, no. 5, pp. 413–422, 2008.

[5] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, 2014.

[6] B. Suh and I. Han, "The IS risk analysis based on a business model," *Inf. Manage.*, vol. 41, no. 2, pp. 149–158, 2003.

[7] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis," *Inf. Sci.*, vol. 256, pp. 57–73, Jan. 2014.

[8] M. E. Whitman and H. J. Mattord, *Management Of Information Security, 2/E*. Boston, MA, USA: Course Technology Press, 2007.

[9] M. S. Saleh and A. Alfantookh, "A new comprehensive framework for enterprise information security risk management," *Appl. Comput. Inform.*, vol. 9, no. 2, pp. 107–118, 2011.

[10] J. H. P. Eloff and M. Eloff, "Information security management: A new paradigm," in *Proc. Annu. Res. Conf. South African Inst. Comput. Scientists Inf. Technologists Enablement Technol. South African Inst. Comput. Scientists Inf. Technologists*, 2003, pp. 130–136.

[11] M. M. Silva, T. Poleto, L. C. e Silva, A. P. H. de Gusmao, and A. P. C. S. Costa, "A grey theory based approach to big data risk management using FMEA," *Math. Problems Eng.*, vol. 2016, Jul. 2016, Art. no. 9175418.

[12] M. M. Silva, A. P. H. de Gusmão, T. Poleto, L. C. e Silva, and A. P. C. S. Costa, "A multidimensional approach to information security risk management using FMEA and fuzzy theory," *Int. J. Inf. Manage.*, vol. 34, no. 6, pp. 733–740, 2014.

[13] A. P. H. de Gusmão, L. C. e Silva, M. M. Silva, T. Poleto, and A. P. C. S. Costa, "Information security risk analysis model using fuzzy decision theory," *Int. J. Inf. Manage.*, vol. 36, no. 1, pp. 25–34, 2016.

[14] P. Shedden, W. Smith, and A. Ahmad, "Information security risk assessment: Towards a business practice perspective," in *Proc. Aust. Inf. Secur. Manage. Conf.*, 2010, pp. 119–130.

[15] C. Chen, "CiteSpace II: Detecting and visualizing emerging trends and transient patterns in scientific literature," *J. Amer. Soc. Inf. Sci. Technol.*, vol. 57, no. 3, pp. 359–377, 2006.

[16] C. Chen, "Searching for intellectual turning points: Progressive knowledge domain visualization," *Proc. Nat. Acad. Sci. USA*, vol. 101, no. 1, pp. 5303–5310, 2004.

[17] C. Chen, I.-Y. Song, X. Yuan, and J. Zhang, "The thematic and citation landscape of *data and knowledge engineering* (1985–2007)," *Data Knowl. Eng.*, vol. 67, no. 2, pp. 234–259, 2008.

[18] Y. Tonta and G. Düzyol, "Mapping the structure and evolution of electronic publishing as a research field using co-citation analysis," in *Proc. ELPUB, Conf. Electron. Publishing*, 2010.

[19] R. Zhao and J. Wang, "Visualizing the research on pervasive and ubiquitous computing," *Scientometrics*, vol. 86, no. 3, pp. 593–612, 2011.

[20] M. Niazi and A. Hussain, "Agent-based computing from multi-agent systems to agent-based models: A visual survey," *Scientometrics*, vol. 89, p. 479, Nov. 2011.

[21] R. Y. Zhao, M. Wang, Z. H. Dang, Z. Dang, and G. Zhang, "Visual analysis of international oil flax research," *Adv. Mater. Res.*, vols. 343–344, pp. 673–677, Sep. 2010.

[22] G. Liu, "Visualization of patents and papers in terahertz technology: A comparative study," *Scientometrics*, vol. 94, no. 3, pp. 1037–1056, 2013.

[23] Z. Lin, C. Wu, and W. Hong, "Visualization analysis of ecological assets/values research by knowledge mapping," *Acta Ecologica Sinica*, vol. 35, no. 5, pp. 142–154, 2015.

[24] D. Chen, Z. Liu, Z. Luo, M. Webber, and J. Chen, "Bibliometric and visualized analysis of emergy research," *Ecological Eng.*, vol. 90, pp. 285–293, May 2016.

[25] P. Cronin, F. Ryan, and M. Coughlan, "Undertaking a literature review: A step-by-step approach," *Brit. J. Nursing*, vol. 17, no. 1, pp. 38–43, 2008.

[26] E. F. Fama and K. R. French, "Common risk factors in the returns on stocks and bonds," *J. Financial Econ.*, vol. 33, no. 1, pp. 3–56, 1993.

[27] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.

[28] D. W. Straub, Jr., and R. J. Welke, "Coping with systems risk: Security planning models for management decision making," *MIS Quart.*, vol. 22, no. 4, pp. 441–469, 1998.

[29] D. W. Straub, Jr., "Effective is security: An empirical Study," *Inf. Syst. Res.*, vol. 1, no. 3, pp. 255–276, 1990.

[30] R. C. Merton, "On the pricing of corporate debt: The risk structure of interest rates," *J. Finance*, vol. 29, no. 2, pp. 449–470, 1974.

[31] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. Marketing Res.*, vol. 18, no. 1, pp. 39–50, 1981.

[32] M. M. Carhart, "On persistence in mutual fund performance," *J. Finance*, vol. 52, no. 1, pp. 57–82, 1997.

[33] K.-H. Cho, "Continuous auctions and insider trading: Uniqueness and risk aversion," *Finance Stochastics*, vol. 7, no. 1, pp. 47–71, 2003.

[34] F. Black and M. Scholes, "The pricing of options and corporate liabilities," *J. Political Economy*, vol. 81, no. 3, pp. 637–654,1973.

[35] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quart.*, vol. 13, no. 3, pp. 319–340, 1989.

[36] N. Jegadeesh and S. Titman, "Returns to buying winners and selling losers: Implications for stock market efficiency," *J. Finance*, vol. 48, no. 1, pp. 65–91, Mar. 1993.

[37] D. Duffie and K. J. Singleton, "Modeling term structures of defaultable bonds," *Rev. Financial Stud.*, vol. 12, no. 4, pp. 687–720, 1999.

[38] P. Zhang and R. I. Benjamin, "Understanding information related fields: A conceptual framework," *J. Amer. Soc. for Inf. Sci. Technol.*, vol. 58, no. 13, pp. 1934–1947, 2007.

XIAOTONG LI was born in China in 1988. She received the B.S. degree from Dalian Polytechnic University in 2010 and the M.S. degree from Northwest Agriculture and Forestry University in 2014.

She is currently pursuing the Ph.D. degree with the School of Economics and Management, Xidian University. Research interests grey systems theory, fuzzy theory, game theory, information security investment, and sharing.

HUA LI was born in China in 1963. He received the M.S. degree from Shaanxi Normal University in 1991 and the Ph.D. degree from Xidian University in 1999.

He is currently a Professor and a Doctoral Advisor with the School of Economics and Management, Xidian University. He has authored or co-authored more than 20 publications. His research interests include the transformation of scientific and technological achievements, and decision analysis.

• • •