Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.021786
Article

Tech Science Press

Analysis and Intellectual Structure of the Multi-Factor Authentication in Information Security

Rashad Mahmood Saqib[1], Adnan Shahid Khan[1,*], Yasir Javed[2], Shakil Ahmad[2], Kashif Nisar[3], Irshad A. Abbasi[4], Muhammad Reazul Haque[5] and Azlina Ahmadi Julaihi[1]

[1]Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, 94300, Kota Samarahan, Malaysia
[2]Computer and Information Science, Prince Sultan University, Riyadh, KSA
[3]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, 88400, Kota Kinabalu Sabah, Malaysia
[4]Faculty of Computer Science, University of Bisha, Bisha, Saudi Arabia
[5]Faculty of Computing & Informatics, Multimedia University, Persiaran Multimedia, 63100, Cyberjaya, Selangor, Malaysia
*Corresponding Author: Adnan Shahid Khan. Email: skadnan@unimas.my

Received: 14 July 2021; Accepted: 04 October 2021

Abstract: This study presents the current state of research on multi-factor authentication. Authentication is one of the important traits in the security domain as it ensures that legitimate users have access to the secure resource. Attacks on authentication occur even before digital access is given, but it becomes quite challenging with remote access to secure resources. With increasing threats to single authentication schemes, 2Factor and later multi-factor authentication approaches came into practice. Several studies have been done in the multi-factor authentication discipline, and most of them proposed the best possible approaches, but there are very limited studies in the area that can comprehend all these innovative and effective approaches. Using Web of Science data of the research publications on the topic, the study adopted the bibliometric approach to find the evolution of authentication in the security domain, especially multi-factor authentication. This study finds the impact of the research in the selected domain using bibliometric analysis. This research also identifies the key research trends that most of the researchers are paying attention to. The highest number of publications on multi-factor authentication were published in 2019 while the highest number of citations were received in 2014. United States, India, and China are the leading countries publishing the most on multi-factor authentication.

Keywords: Multi-factor authentication; bibliometrics; scient metrics; authentication; information security

1 Introduction

The security domain is getting a lot of attention since the last decade due to the increased number of attacks, reliance on wireless and remote setup, and especially the movement of financial transactions to online mediums. A lot of efforts have been made in the area of security by the introduction of passwords, encryption, hashing, biometric authentication, and the list goes on. Still, lack of security awareness, security loopholes have always been a challenge and resulted in a security compromise. In the current era, two-level or multilevel security is getting a lot of attention where multiple factors are considered for implementing security. In this way, security can be ensured to mitigate attacks caused by human carelessness, lack of awareness, and other bot attacks to protect sensitive data from possible security attacks [1–6] like distributed denial of service (DDoS) attacks [7–10] as the first line of defense. Furthermore, information security is big factor to implement internet of things (IoT) for smart cities [11–19] using software-defined networking [SDN] [20–26], named data networking (NDN) [27–29] and cloud computing network [30] with voice over IP (VoIP) [31–34] fiber optic [35–37], worldwide interoperability for microwave access (WiMAX) [37–40], swarm intelligence (SI) [41], artificial intelligence (AI), machine learning (ML) [42], deep learning (DL) [42–44], and artificial neural network (ANN) [45].

Legitimate access to any resource requires authentication of the person accessing the protected resource [46]. Usually, this protection is done through a username and password which if, compromised, may result in total failure of the system. It can easily be comprehended by considering if someone can sneak into your mobile phone, and the only security provided is a passcode or pin. Biometric, a common authentication scheme, was introduced as a replacement to the password that ensures that a legitimate person is logging. However, it can be compromised as the famous case of Apple Hack in 48 h in a security conference in Germany [47]. Two-factor authentication was introduced where the combination of password and biometric was preferred to be used as it provide chances to have better security. This research focuses on finding the evolution of different authentication schemes and how different combinations of authentication schemes are used to form multi-factor authentication schemes [48].

Several studies and authentication schemes are currently in use for providing legitimate access to the protected resources. Each scheme has its pros and cons making it challenging to adapt in every possible scenario. This results in a multiple-level authentication scheme based on the nature of the resource [47–50]. The following section presents the common authentication schemes and how they are used.

Password: Usage of password or pin or even passcode is one of the oldest mechanisms for protecting resources from legitimate access. Passwords are considered secure; based on their size and complexity. But the number of passwords released over the dark web as well as other compromises has resulted in failure of the scheme or even, in some cases, ransom or maligning of person. Secondly, if a password is compromised, the whole security scheme becomes null and void [51].

Biometric: Several biometric schemes are used for providing authentication such as facial recognition, fingerprint, and iris authentication. It allows guarantee of real and legitimate human access but advances in the recreation of images, biometric has resulted in the compromise of the scheme [52].

One Time Password (OTP): OTP scheme is widely used these days as it allows live access to resources using a fresh password. Usually, OTP is used in conjunction with other authentication schemes but still can be compromised using a Man-in-the-Browser attack or malware [53].

Smartcard: Barkadehi et al. and Velásquez et al. discussed that smart cards are often used to provide security and authentication by keeping the secret information protected. It is widely used to authenticate resources smartly and efficiently. But it is complex to handle because it may be lost or stolen to resources; also, indirect gains and rouge relay attacks are possible.

Blind-Fold Challenge Scheme: Owing to the increased number of bot attacks, currently verification of human factor has been introduced by random challenges such as identification of the object in the picture, captcha, easy math equation or set of challenges but still with advances in image recognition made it possible to crack captcha, it is challenging for blind or low sight user to use complex scheme. Secondly the blindfold challenge scheme cannot be used as security scheme it only distinguishes humans from machines [53–55].

Profiling: Security profiling of users is often considered to be an adaptive authentication scheme where a user profile is completely built, and whenever a slight deviation is considered from normal behavior, complex authentication schemes are introduced again. This scheme results in fast access and ensures legitimate users are using the resources but, in some cases, due to an emergency, if the user is behaving abnormally all of the access may get blocked and may result in some serious injury. Profiling can be location-based, timing-based, device type, or even connection-based. All of them can be used in conjunction with other approaches to achieve better security [55–57].

MFA works on three major principles (1) knowledge: what you know such as your pin, password, etc. (2) possession: an asset that you have in hand such as a mobile phone and (3) inherence that refers to what is unique to you such as biometric information [58]. A better approach must use all these three together based on the level of security that resource requires. This research adopts bibliometric analysis to find out how multifactor is analyzed in scientific literature and which principles are covered in these approaches. Bibliometric analysis is a statistical approach evaluate the published scientific literature. There are several studies that have been conducted using bibliometric studies in the area of security and authentication schemes, but very limited studies have been done in the area of multifactor authentication. [59] conducted a bibliometric study about authentication that covered a variety of security and the Internet of Things (IoT). [60] researched around smart grid and Internet of Things security. Both pieces of research investigate publications made in a vast area and provide a highlight of keywords for consideration also. [61] conducted a bibliometric study on security and application of bibliometric, while [62] conducted a bibliometric study for how security is analyzed in the blockchain. There are few studies about security such as [63–67] analyzed the security issues using bibliometric studies and extracted the major publication patterns. MFA is not a new research area, but the real usage came with a number of security issues on a rise. Security experts worked on approaches that include MFA but there is a lack of studies that can comprehend what has been done in area and what are the current researches heading too.

The main objective of this study is to present the current state of research on multi-factor authentication. To achieve the stated objective, the study aimed to answer the following research questions interpreting the scope of the research as well.

- How have the research publications and citations on multi-factor authentication evolved over time?
- What is the impact and citation structure of the research on multi-factor authentication?
- What are the research trends in multi-factor authentication in terms of authorship patterns, active countries, institutions, journals and researchers?
- What are the main themes in the domain and how have these themes evolved over time?
- What are the recent research trends in this domain?

2 Methodology of the Research

2.1 Bibliometric Terminology

This study used bibliometric terminology and abbreviations as under Tab. 1.

Active authors, institutions and countries are those with the highest number of publications.

2.2 Tools Used

Gephi, an open-source tool was used to visualize the keywords co-occurrences, present co-citation graphs, and create the bibliometric coupling. Thematic evolution and collaboration trends were explored using another open-source tool Biblioshiny [68–70], version 2.0. Microsoft Excel was used to scan the titles and abstracts.

Table 1: Bibliometric terminology and abbreviations

Abbreviation/terminology	Full form/explanation
TP	total citations
TC	total citations
PY	publication year
NCP	number of cited publications
(C/P)	average citations per publication
C/CP	average citations per cited publication
CPY	average citations per year
H	h-index
IF impact factor	impact factor
CoL	co-citation links

2.3 Data Source

The selection of a database is an important task in bibliometric studies. Web of Science (WoS) was selected to retrieve data as it is one of the most comprehensive and premier citations and abstract databases of scientific literature in the selected domain. WoS indexes the relevant, authoritative and top-ranked journals and has a wider coverage of scholarly literature on computer security and allied subject domains.

2.4 Method

Bibliometric method of research analysis was applied to conduct this study. The method is widely used in evaluating the research performance in particular fields of knowledge, institutions, regions and journals.

2.5 Search Query and Data Retrieval

To retrieve the bibliographic and citation records of "multi-factor authentication" a search query with the keyword "Multi-factor authentication" was run in the "Topic" field in the Web of Science Core Collection. The topic field brings results from the title, keywords, and abstracts of the publications. The search was performed on February 22, 2021. Two of the authors retrieve the data simultaneously to validate the retrieved data. The titles and abstracts of the results were scanned to check their relevancy.

3 Analysis, Results and Discussion

In this section, data analysis, and results have presented with analytical discussion.

3.1 Evolution of Publications and Citations in Multi-Factor Authentication

Fig. 1 explains the chronological growth of publications and citations in the multi-factor authentication domain. Data indicated a gradual increase in the multi-factor authentication publications and citations with minor fluctuations. The first publication on the topic appeared in 2004, while the year 2019 witnessed the highest number of publications (n = 55). The highest number of citations (n = 240 and n = 154) were received in the years 2014 and 2015, respectively. The citation structure provided in Tab. 2 revealed that the highest number of cited publications were in 2019, while the best average citation per publication and the average citations per cited publications were observed in the publications in the year 2014. The best h-index of six (6) was recorded to the publications in the years 2014, 2015, 2016.

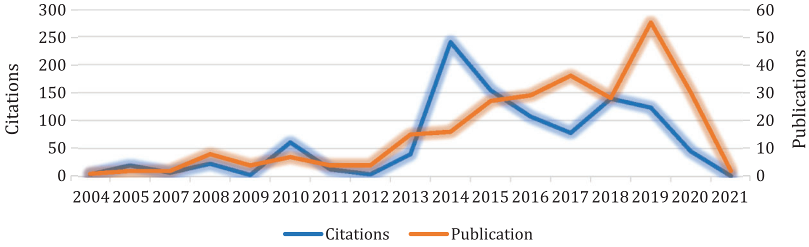


Figure 1: Publications and citation trends

Table 2: Citation structure of multi-factor authentication publications between 2004 and 2021

PY	TP	TC	NCP	C/P	C/CP	H-index
2004	1	4	1	4.00	4.00	1
2005	2	20	2	10.00	10.00	2
2007	2	7	2	3.50	3.50	2
2008	8	23	3	2.88	7.67	3
2009	4	3	2	0.75	1.50	1
2010	7	61	7	8.71	8.71	3
2011	4	13	2	3.25	6.50	2
2012	4	4	2	1.00	2.00	2
2013	15	40	8	2.67	5.00	3
2014	16	240	11	15.00	21.82	6
2015	27	154	18	5.70	8.56	6
2016	29	107	17	3.69	6.29	6
2017	36	78	23	2.17	3.39	5
2018	28	139	14	4.96	9.93	5
2019	55	123	28	2.24	4.39	5
2020	30	45	13	1.50	3.46	4
2021	2	1	1	0.50	1.00	1

3.2 Active Countries and Institutions

Data in Tab. 3 indicates that the United States is the most active country publishing research in multi-factor authentication with 49 publications, followed by India and China with 40 and 31 publications, respectively. The best citation impact of 15.50 was recorded to the publications affiliated with Australian institutions. Purdue University, Tampere University of Technology, ITMO University, The University of Buckingham, and Mimos Berhad published four publications each on the topic. Publications of Wuhan University attracted the highest number of citations (135) and created the best citation impact of 45 among the top active institutions. Purdue University followed Wuhan University in getting the second most (75) citations.

Table 3: Leading countries and institutions

Top 10 countries					Top 10 organizations				
Rank	Country	TP	TC	CI	Rank	Organization	TP	TC	CI
1	United States	49	273	5.57	1	Purdue University	4	75	18.75
2	India	40	203	5.08	2	Tampere University of Technology	4	39	9.75
3	China	31	289	9.32	3	ITMO University	4	34	8.50
4	South Korea	27	191	7.07	4	The University of Buckingham	4	5	1.25
5	England	22	185	8.41	5	Mimos Berhad	4	3	0.75
6	Malaysia	11	16	1.45	6	Fondazione Bruno Kessler	3	3	1.00
7	Russia	9	40	4.44	7	Fujian Normal University	3	71	23.67
8	Australia	8	124	15.50	8	Georgia Institute of Technology	3	14	4.67
9	Brazil	7	11	1.57	9	Korea Advanced Institute of Science and Technology	3	14	4.67
10	Czech Republic	7	8	1.14	10	Wuhan University	3	135	45.00

3.3 Influential Journals

IEEE Access was the most active journal publishing research on multi-factor authentication. Most of the journals presented in Tab. 4 are impact factor journals listed in Journal Citation Reports of Clarivate Analytics. The majority of these journals are ranked in the first and second quartiles of journal rankings. All of the top ten journals are based in the United States and European countries.

Table 4: Most influential journals publishing research on multi-factor authentication

Rank	Journal	TP	TC	IF	Q	Publisher	Country
1	IEEE Access	7	3	3.745	1	IEEE	United Sates
2	Multimedia Tools and Applications	4	8	2.313	2	Springer	Netherlands
3	Computers & Security	4	33	3.579	2	Elsevier	England
4	Cryptography	3	23	NA	NA	MDPI	Switzerland
5	International Journal of Advanced Computer Science and Applications	3	1	NA	NA	Science and Information Organization	England
6	IEEE Transactions on Dependable and Secure Computing	3	78	6.864	1	IEEE Computer Society	United Sates
7	IEEE Network	2	32	8.808	1	IEEE	United Sates
8	IET Information Security	2	19	1.068	3	Wiley	United Sates
9	Information and Software Technology	2	22	2.726	2	Elsevier	Netherlands
10	Computer Networks	2	16	3.111	2	Elsevier	Netherlands

3.4 Most Cited Manuscripts in the Multi-Factor Authentication Domain

Tab. 5 lists the top ten manuscripts that have received the highest number of citations. The manuscript titled "Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices", (He, Debiao, 2014), published in IEEE Transactions on Consumer Electronics, received the highest number of citations (107), with an average of 15.29 citations annually. The article titled "Molecules for security measures: from keypad locks to advanced communication protocols" (Andreasson, J. 2018), published in Chemical Society Reviews, received the best average of 19 citations per year.

Table 5: Highly cited articles in multi-factor authentication domain

Rank	Title	First Author	Journal	PY	TC	CPY
1	Enhanced Three-factor Security Protocol for Consumer USB Mass Storage Devices	He, Debiao	IEEE Transactions on Consumer Electronics	2014	107	15.29
2	Robust Multi-Factor Authentication for Fragile Communications	Huang, Xinyi	IEEE Transactions on Dependable and Secure Computing	2014	68	9.71
3	Molecules for security measures: from keypad locks to advanced communication protocols	Andreasson, J.	Chemical Society Reviews	2018	57	19.00
4	Secure biometric template generation for multi-factor authentication	Khan, Salman H.	Pattern Recognition	2015	48	8.00
5	Combining Fuzzy Extractor in Biometric-Kerberos based Authentication Protocol	Thi Ai Thao Nguyen	2015 International Conference on Advanced Computing and Applications	2015	43	7.17
6	Usable security: User preferences for authentication methods in eBanking and the effects of experience	Weir, Catherine S.	Interacting with Computers	2010	35	3.18
7	Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem	Chan, Aldar C.-F.	IEEE Journal on Selected Areas in Communications	2014	26	3.71
8	CNN-based anti-spoofing two-tier multi-factor authentication system	Sajjad, Muhammad	Pattern Recognition Letters	2019	24	12.00
9	Multi-Factor Authentication: A Survey	Ometov, Aleksandr	Cryptography	2018	21	7.00
10	Authentication and Authorization Mechanisms for Substation Automation in Smart Grid Network	Vaidya, Binod	IEEE Network	2013	19	2.38

3.5 Authorship Pattern

Most of the research on multi-factor authentication is done collaboratively, as indicated in Fig. 2. Three-author studies are the most common trend followed by the studies prepared by joint effort of two authors.

Seventeen studies were prepared by single authors. Studies prepared in collaboration received citations with better a average than the single-author studies. Studies with eight authors were cited with an average of 12 citations per publication. The second-best citation average of 7. 5 was recorded to the publications with five authors. Single author studies received the lowest citation average of 2 citations per publication.

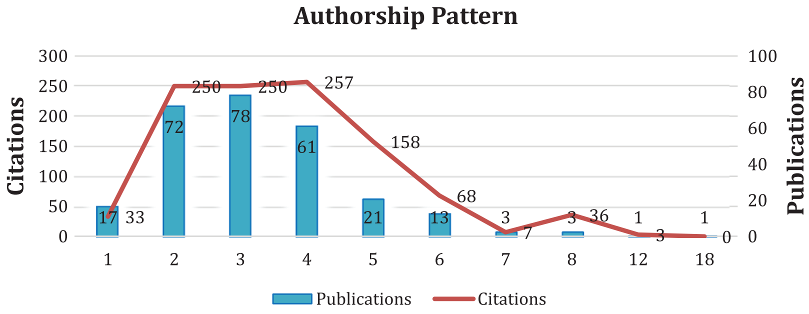


Figure 2: Authorship pattern of multi-factor authentication publications

3.6 Co-occurrences Analysis of Keywords

Using Gephi software, the co-occurrences of author-supplied keywords were analyzed. The keywords with a minimum of four assurances were selected to appear in Fig. 3; 28 keywords met the threshold. Fig. 3 shows interesting co-relations between the author keywords indicating connections to multi-factor authentication. Based on the weight of co-occurrences and total link strength, multi-factor authentication was the most frequently used keyword establishing its connections to biometrics, security, and authentication. Seven different colors represent seven clusters.

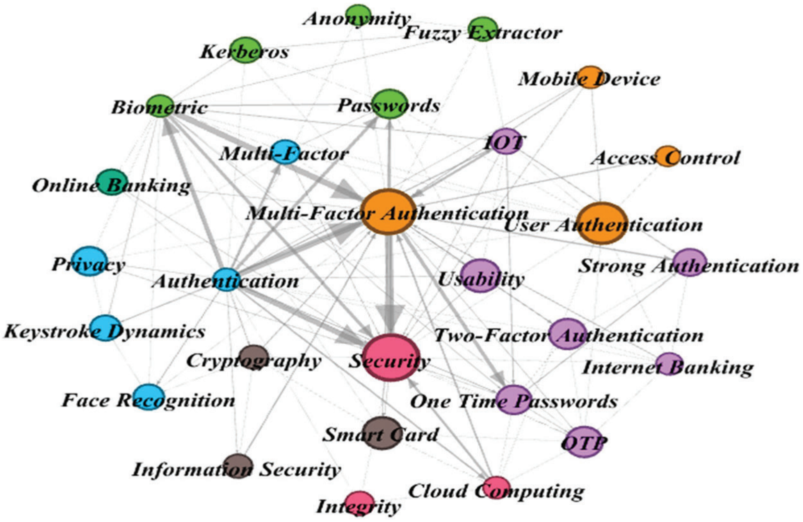


Figure 3: Keywords co-occurrences of manuscripts published in multi-factor authentication domain

3.7 Bibliographic Coupling of the Countries of the Authors

Fig. 4 presents the bibliographic coupling of the countries of the authors of multi-factor authentication articles. A threshold of five publications was set. Nineteen countries met the criteria and appeared on the coupling map. The United States had the best strength based on the number of publications, while China was on the top based on the total link strength and citations. The nodes in Fig. 4 represent the countries, while the edges represent the network. The width of the edge indicates the association level. The color of the nodes represents the clusters.

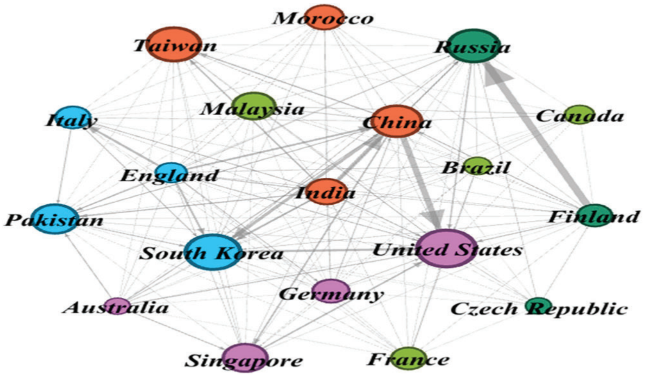


Figure 4: Bibliographic coupling of authors affiliated countries

3.8 Bibliographic Coupling of the Authors' Affiliated Institutions

Fig. 5 shows the bibliographic coupling of the institutions of the authors who are publishing on multi-factor authentication. With the threshold of three publications, fifteen institutions qualified to appear on the coupling map. The representation of institutions from around the world indicates that research on multi-factor authentication is being carried out globally. A strong collaboration can be observed between the ITMO University and the Tempere University of Technology.

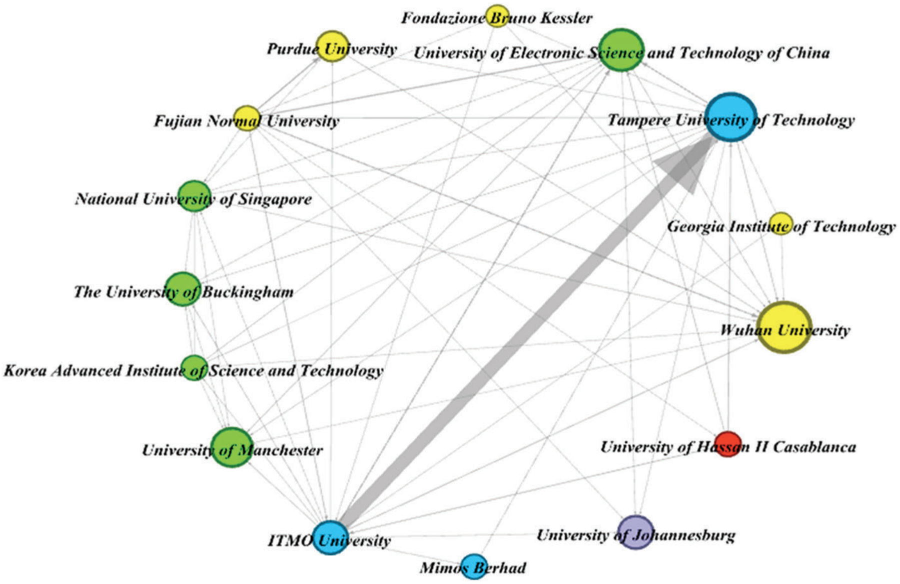

Fondazione Bruno Kessler
Purdue University
University of Electronic Science and Technology of China
Fujian Normal University
Tampere University of Technology
National University of Singapore
Georgia Institute of Technology
The University of Buckingham
Wuhan University
Korea Advanced Institute of Science and Technology
University of Manchester
University of Hassan II Casablanca
University of Johannesburg
ITMO University
Mimos Berhad

Figure 5: Bibliographic coupling of organizations

3.9 Three-Field Analysis of Keywords, Countries and Journals

Fig. 6 shows a three-field plot of keywords (left), countries (center), and journals (right), identifying the relationship among the keywords, countries, and journals. "Multi-factor authentication" and "authentication" keywords were the most frequently used keywords, as indicated by the size of the boxes. India, China, and

United States are using these keywords the most, while the journals IEEE Access, and Computers and Society have published most of the research on these keywords.

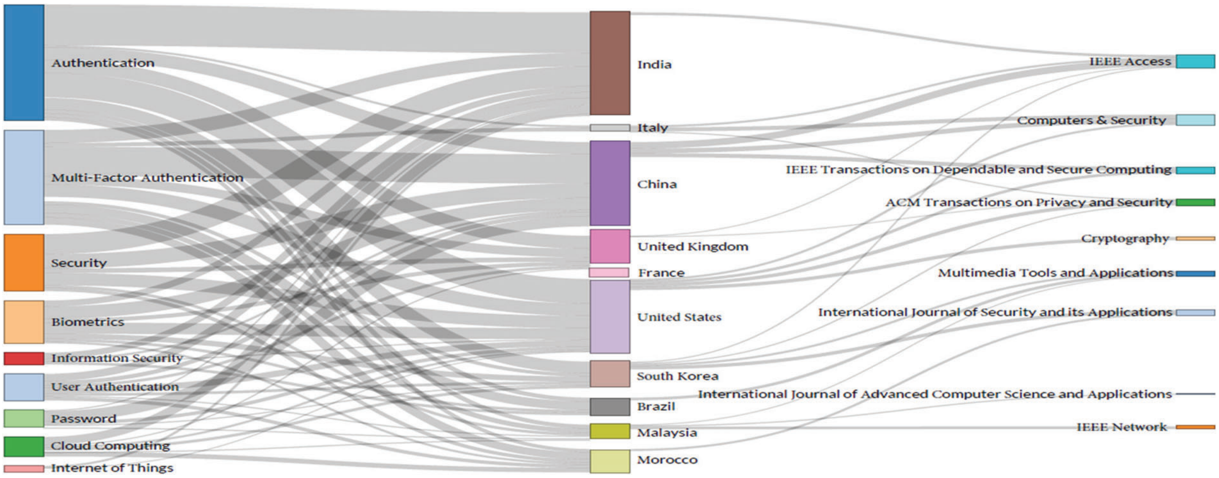


Figure 6: Three-field plot of keywords, countries and journals

3.10 Thematic Evolution of Keywords

Fig. 7 presents the thematic evolution of keywords used in the multi-factor authentication research. The temporal analysis was made on the main themes of the domain that divides the research life span over three different time slices. Results indicate that multi-factor authentication, password, and authentication were the popular keywords since the emergence of the field. Confidentiality, biometrics, and security were the new areas of focus from 2016 to 2018. Behavior, OTP, anonymity, and information security emerged as the new research themes during the last two years. Multi-factor authentication has been the focus of research throughout the lifespan of the field.

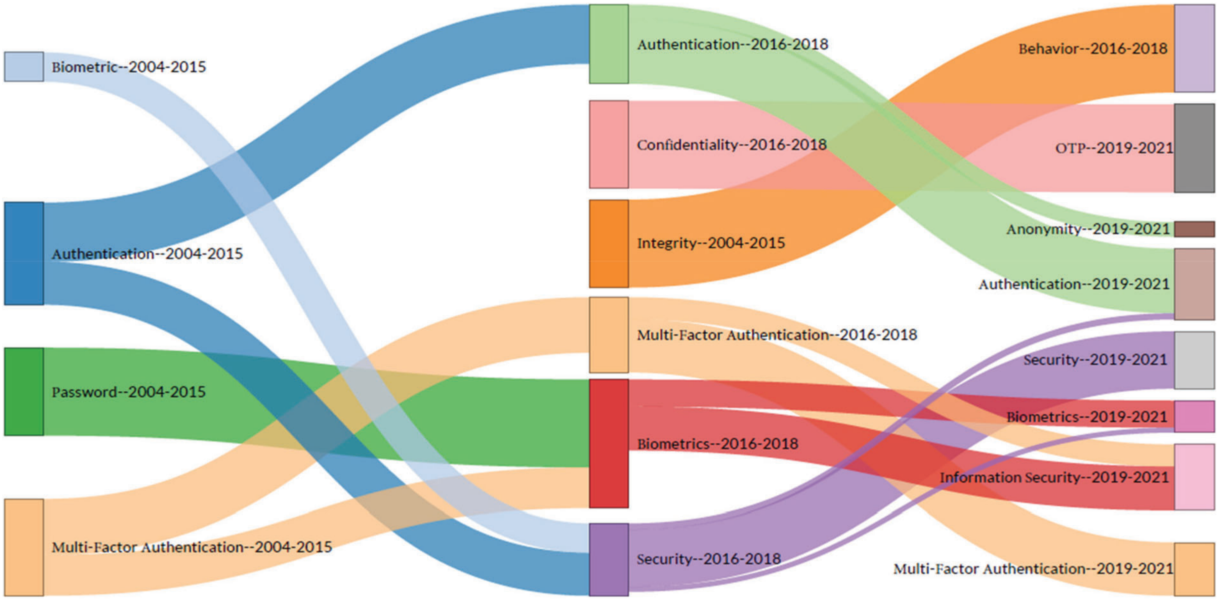
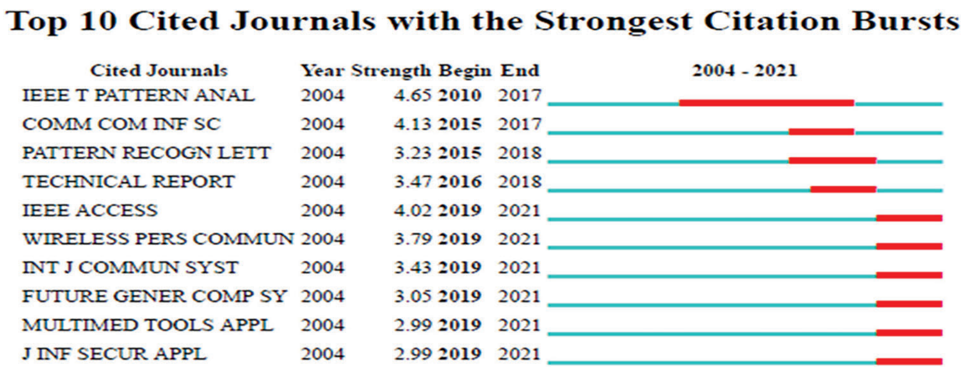


Figure 7: Thematic evolution of keywords used in multi-factor authentication research

3.11 *Journals with the Best Citation Bursts*

Fig. 8 presents the citation bursts on the journals publishing research on mulita-factor authentication. The strongest citation burst with the burst strength of 4.65 was recorded to the IEEE Transactions on Pattern Analysis and Machine Intelligence. The burst lasted for eight years, from 2010 to 2017. The other journals with the notable bursts were Communications in Computer and Information Science and IEEE Access with the burst strengths of 4.13 and 4.02, respectively.



Top 10 Cited Journals with the Strongest Citation Bursts

Cited Journals	Year	Strength	Begin	End	2004 - 2021
IEEE T PATTERN ANAL	2004	4.65	2010	2017	
COMM COM INF SC	2004	4.13	2015	2017	
PATTERN RECOGN LETT	2004	3.23	2015	2018	
TECHNICAL REPORT	2004	3.47	2016	2018	
IEEE ACCESS	2004	4.02	2019	2021	
WIRELESS PERS COMMUN	2004	3.79	2019	2021	
INT J COMMUN SYST	2004	3.43	2019	2021	
FUTURE GENER COMP SY	2004	3.05	2019	2021	
MULTIMED TOOLS APPL	2004	2.99	2019	2021	
J INF SECUR APPL	2004	2.99	2019	2021	

Figure 8: Top ten cited journals with the strongest citation bursts

4 Limitations and Future Research Directions

The data source of this study is WoS database. Other citations and abstract databases such as Scopus, Google Scholar may reflect a different number of publications and citations on MFA. The study used the "multi-factor authentication" keyword to search for and retrieve the data. Other keywords will yield other results as databases retrieve a different set of records with the change of keywords. A systematic review of MFA will be a good source of knowledge for the researchers in the field. A bibliometric study using the other abstract and indexing databases to map the current research landscape of MFA will be a good addition to the current literature in the domain. A comparative study of different regions and countries can be carried out that may reflect on priorities or, even in some cases, weakness in the domain. The same study can select best and effective practices to create a general framework for effective multi-factor authentication schemes.

5 Conclusion

Authentication is an essential aspect of security and has always gained attention as well as attacks over time. This research study focuses on MFA that was coined a long time ago as two-factor or three-factor authentication. The selected data source shows 2004 when it received an approach comprising of MFA and then a steady increase was observed. It was a decade after when MFA gained more popularity and impact, as shown through citation analysis, that was due to the usage of intelligent approaches for compromising the authentication. The United States, India, and China were the most active countries publishing MFA research, while Purdue University was the most prolific institution. The highest number of studies were published in IEEE Access. Researchers preferred to conduct their research collaboratively. MFA, biometrics, security, and authentication were the most frequently used keywords. Behavior, OTP, anonymity, and information security emerged as the new research themes during the last two years, while confidentiality, biometrics, and security were the areas of focus from 2016 to 2018. The study recommends future researchers conduct a systematic literature review on the topic to uncover the research on MFA in terms of security approaches adapted.

Acknowledgement: The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication. The authors would like to thank the editors of IASC and anonymous reviewers for their time and review of this manuscript and Professor Dr. Yong-Jin Park (IEEE Life member and former Director IEEE Region 10) valuable comments and suggestions on improving the paper.

Funding Statement: This research is funded by Prince Sultan University and Research, Innovation and Enterprise Centre (RIEC), Universiti Malaysia Sarawak under the Grant No. F08/PGRG/2058/2021, Y. Javed and A. S. Khan received the grant, sponsors' websites: https://www.riec.unimas.my.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32. no. 1, pp. 4150–4179, 2021.

[2] M. S. Dildar, N. Khan, J. B. Abdullah and A. S. Khan, "Effective way to defend the hypervisor attacks in cloud computing," in *2nd Int. Conf. on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, pp. 154–159, 2017.

[3] A. S. Khan, Y. Javed and J. Abdullah, "Trust-based lightweight security protocol for device to device multihop cellular communication (TLwS)," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 1–18, 2021.

[4] A. S. Khan, K. Balan, Y. Javed, J. Abdullah and S. Tarmizi, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors (Switzerland)*, vol. 19, no. 22, pp. 1–27, 2019.

[5] S. O. Maikol, A. S. Khan, Y. Javed, A. L. A. Bunsu, C. Petrus *et al.,* "A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities," *International Journal of Integrated Engineering*, vol. 13, no. 2, pp. 127–135, 2020.

[6] I. A. Abbasi, A. S. Khan and S. Ali, "A reliable path selection and packet forwarding routing protocol for vehicular ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, no. 236, pp. 1–19, 2018.

[7] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* "Automated controller placement for software-defined networks to resist DDoS attacks," *Computers, Materials & Continua*, Tech Science Press, Henderson, Nevada, USA, vol. 68, no. 3, pp. 3147–3165, 2021.

[8] A. S. Khan, H. Lenando, J. Abdullah and N. Fisal, "Secure authentication and key management protocols for mobile multihop wimax networks," *Jurnal Teknologi*, vol. 73, no. 1, pp. 75–81, 2015.

[9] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, R. Kaspin *et al.,* "Unprecedented smart algorithm for uninterrupted SDN services during DDoS attack," *Computers, Materials & Continua*, Tech Science Press, Henderson, Nevada, USA, vol. 70, no. 1, 2022.

[10] A. S. Khan, Z. Ahmad, J. Abdullah and F. Ahmad, "A spectrogram image-based network anomaly detection system using deep convolutional neural network," *IEEE Access*, vol. 9, no. 1, pp. 87079–87093, 2021.

[11] I. Haider, K. B. Khan, M. A. Haider, A. Saeed and K. Nisar, "Automated robotic system for assistance of isolated patients of coronavirus (COVID-19)," in *IEEE 23rd Int. Multitopic Conf. (INMIC)*, Bahawalpur, Pakistan, pp. 1–6, 2020.

[12] K. Balan, A. S. Khan, A. A. Julaihi, S. Tarmizi and K. S. Pillay "RSSI and public key infrastructure based secure communication in autonomous vehicular networks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 12, pp. 298–304, 2018.

[13] N. I. Sarkar, A. X. Kuang, K. Nisar and A. Amphawan, "Performance studies of integrated network scenarios in a hospital environment," *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, vol. 6. no. 1, pp. 35–68, 2014.

[14] N. I. Sarkar, A. X. Kuang, K. Nisar and A. Amphawan, "Hospital environment scenarios using WLAN over OPNET simulation tool," *International Journal of Information Communication Technologies and Human Development (IJICTHD)*, vol. 6. pp. 69–90, 2014.

[15] B. Chowdhry, A. A. Shah, N. Harris, T. Hussain and K. Nisar, "Development of a smart instrumentation for analyzing railway track health monitoring using forced vibration," in *IEEE 14th Int. Conf. on Application of Information and Communication Technologies (AICT)*, Tashkent, Uzbekistan, pp. 1–5, 2020.

[16] K. Nisar and A. I. Saudi "Smart home: Multisensor information fusion towards better healthcare," *Advanced Science Letters*, vol. 24, no. 3, pp. 1896–1901, 2018.

[17] N. Khan, J. Abdullah and A. S. Khan, "Defending malicious script attacks using machine learning classifiers," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–9, 2017.

[18] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* "SDN architecture for UAVs and EVs using satellite: A hypothetical model and new challenges for future," in *IEEE 18th Annual Consumer Communications & Networking Conf. (CCNC)*, Las Vegas, NV, USA, pp. 1–6, 2021.

[19] K. Nisar, E. R. Jimson, M. H. A. Hijazi and S. K. Memon "A survey: Architecture, security threats and application of SDN," *Journal of Industrial Electronics Technology and Application*, Daegu University, Republic of Korea, vol. 2, no. 1, pp. 64–69, 2019.

[20] K. Nisar, G. Chen and A. Sarrafzadeh, "A review: Software defined networks management," in *Network Research Workshop, Proc. of the Asia-Pacific Advanced Network (APAN)*, Fukuoka, Japan, vol. 39, pp. 1–09, 2015.

[21] N. F. Ali, A. M. Said, K. Nisar and I. A. Aziz, "A survey on software defined network approaches for achieving energy efficiency in wireless sensor network," in *IEEE Conf. on Wireless Sensors (ICWiSe)*, Miri, Malaysia, pp. 28–33, 2017.

[22] K. Nisar, M. H. A. Hijazi and A. A. A. Ibrahim, "A new model for virtual machine migration with software defined networking," in *the Fourth Int. Conf. on Computing Science, Computer Engineering, and Education Technologies (CSCEET2017)*, Beirut, Lebanon, 2017.

[23] N. Khan, J. Abdullah and A. S. Khan, "A dynamic method of detecting malicious scripts using classifiers," *Advanced Science Letters*, vol. 23, no. 6, pp. 5352–5355, 2017.

[24] M. R. Haque, S. C. Tan, C. K. Lee, Z. Yusoff, S. Ali *et al.,* "Analysis of DDoS attack-aware software-defined networking controller placement in Malaysia," In: Alja'am J., El Saddik A., Sadka A. (eds.) *In Recent Trends in Computer Applications*, Springer International Publishing AG, Springer Nature, Cham, Switzerland, vol. 1, no. 1, pp. 175–188, 2018.

[25] E. R. Jimson, K. Nisar and M. H. A. Hijazi, "The state of the art of software defined networking (SDN) issues in current network architecture and a solution for network management using the SDN," *International Journal of Technology Diffusion, (IJTD)*, IGI Global Publishers, USA, vol. 10, no. 3, pp. 33–48, 2019.

[26] A. A. A. Ibrahim and K. Nisar, "Future internet and named data networking hourglass, packet and node architecture," *Journal of Industrial Information Technology and Application*, Daegu University, Republic of Korea, vol. 2, no. 3, pp. 115–123, 2018.

[27] S. Zubair, N. Fisal, M. B. Abazeed, B. A. Salihu and A. S. Khan, "Lightweight distributed geographical: A lightweight distributed protocol for virtual clustering in geographical forwarding cognitive radio sensor networks," *International Journal of Communication Systems*, vol. 28, no. 1, pp. 1–18, 2015.

[28] S. Harada, Z. Yan, Y. Park, K. Nisar and A. A. A. Ibrahim, "Data aggregation in named data networking," *IEEE Region 10 Conference (TENCON)*, Malaysia, pp. 1839–1842, 2017.

[29] I. A. Abbasi and A. S. Khan, "A review of vehicle to vehicle communication protocols for VANET in the urban environment," *Future Internet*, vol. 10, no. 14, pp. 1–15, 2018.

[30] K. Nisar, A. Amphawan, S. Hassan and N. I. Sarkar, "A comprehensive survey on scheduler for VoIP over WLANs," *Journal of Network and Computer Applications, (JNCA)*, Norman, OK, USA, vol. 36, no. 2, pp. 933–948, 2013.

[31] F. Sattar, M. Hussain and K. Nisar, "A secure architecture for open source VoIP solutions," in *Int. Conf. on Information and Communication Technologies*, Pakistan, pp. 1–6, 2011.

[32] K. Nisar, A. M. Said and H. Hasbullah, “Enhanced performance of packet transmission using system model over VoIP network,” in *Int. Symposium on Information Technology (ITSim0)*, Kuala Lumpur, Malaysia, pp. 1005–1008, 2010.

[33] N. I., Sarkar, K. Nisar and L. Babbage, “Performance studies on campus-wide focus on ftp, video and VoIP ethernet network,” *International Journal of Advanced Pervasive and Ubiquitous Computing, (IJAPUC)*, IGI Global Publishers, USA, vol. 4, no. 1, pp. 49–59, 2012.

[34] S. Chaudhary, A. Amphawan and K. Nisar, “Realization of free space optics with OFDM under atmospheric turbulence,” *Optik*, vol. 125, no. 18, pp. 5196–5198, 2014.

[35] A. Amphawan, V. Mishra, K. Nisar and B. Nedniyom, “Real-time holographic backlighting positioning sensor for enhanced power coupling efficiency into selective launches in multimode fiber,” *Journal of Modern Optics*, Taylor & Francis Group, UK, vol. 59, no. 20, pp. 1745–1752, 2012.

[36] A. S. Khan, A. Johari, N. Khan, A. Julahi and S. Tarmizi, “Quantum-elliptic curve cryptography for multihop communication in 5G networks,” *International Journal of Computer Science and Network Security*, vol. 17, no. 5, pp. 357–365, 2017.

[37] H. Xiaolong, Z. Huiqi, Z. Lunchao, S. Nazir, D. Jun *et al.,* “Soft computing and decision support system for software process improvement: A systematic literature review,” *Scientific Programming*, vol. 2021, pp. 1–14, 2021.

[38] I. A. Lawal, A. M. Said, K. Nisar and A. A. Mu'azu, “A distributed QoS-oriented model to improve network performance for fixed WiMAX,” *International. Journal on Recent Trends in Engineering and Technology, Association of Computer Electronics and Electrical Engineers, ACEEE*, vol. 10, no. 1, pp. 186–202, 2014.

[39] I. A. Lawal, A. M. Said, K. Nisar, P. A. Shah and A. A. Mu'azu, “Throughput performance improvement for VoIP applications in fixed WiMAX network using client–server model,” *Journal of Science International-Lahore*, Pakistan, vol. 26, no. 3, pp. 999–1002, 2014.

[40] S. Pervaiz, W. H. Bangya, A. Ashraf, K. Nisar, M. R. Haque *et al.,* “Comparative directions of particle swarm optimization algorithms using online networking database,” *Intelligent Automation & Soft Computing*, Tech Science Press, Henderson, Nevada, USA, 2021.

[41] M. R. Haque, S. C. Tan, Z. Yusoff, K. Nisar, C. K. Lee *et al.,* “A novel DDoS attack-aware smart backup controller placement in SDN design,” *Annals of Emerging Technologies in Computing*, London, UK, vol. 4, no. 5, pp. 75–92, 2020.

[42] N. Salam, M. K. Abbas, M. K. Maheshwari, B. Chowdhry and K. Nisar, “Future mobile technology: Channel access mechanism for LTE-LAA using deep learning,” in *IEEE 18th Annual Consumer Communications & Networking Conf. (CCNC)*, USA, pp. 1–5, 2021.

[43] I. A. Abbasi, A. S. Khan and S. Ali “Dynamic multiple junction selection based routing protocol for VANETs in city environment,” *Applied Sciences*, vol. 8, no. 5, pp. 1–18, 2018.

[44] K. Nisar, Z. Sabir, M. A. Z. Raja, A. A. A. Ibrahim, F. Erdogan *et al.,* “ “Design of morlet wavelet neural network for solving a class of singular pantograph nonlinear differential models,” *IEEE Access*, vol. 9, no. 1, pp. 77845–77862, 2021.

[45] T. Y. C. Woo and S. S. Lam, “Authentication for distributed systems,” *Computer*, vol. 25, no. 3, pp. 10, 1992.

[46] M. Bay, “The ethics of unbreakable encryption: Rawlsian privacy and the San Bernardino iPhone,” *First Monday*, vol. 22, no. 2, pp. 1–14, 2017.

[47] B. R. Cha, S. H. Lee, S. B. Park, G. K. Lee and Y. K. Ji, “Design of micro-payment to strengthen security by 2 factor authentication with mobile & wearable devices,” in *the Proc. of Security, Reliability, and Safety*, Delft, Netherland, pp. 28–32, 2015.

[48] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Z. Fardi and S. Samad, “Authentication systems: A literature review and classification,” *Telematics and Informatics*, vol. 35, no. 5, pp. 1491–1511,. 2018.

[49] I. Velásquez, A. Caro and A. Rodríguez, “Authentication schemes and methods: A systematic literature review,” *Information and Software Technology*, vol. 94, pp. 30–37, 2018.

[50] A. Conklin, G. Dietrich and D. Walz, “Password-based authentication: A system perspective,” in *Proc. of the Hawaii Int. Conf. on System Sciences*, Big Island, Hawaii, vol. 37, pp. 2645–2654, 2004.

[51] D. Bhattacharyya, R. Ranjan and M. Choi, “Biometric authentication: A review,” *International Journal of Service, Science and Technology*, vol. 2, no. 3, pp. 13–28, 2009.

[52] M. H. Eldefrawy, K. Alghathbar and M. K. Khan, “OTP-Based two-factor authentication using mobile phones,” in *Proc. 8th Int. Conf. on Information Technology: New Generations, ITNG*, Las Vegas, Nevada, USA, pp. 327–331, 2011.

[53] K. Y. Chan, J. Abdullah and A. S. Khan, “A framework for traceable and transparent supply chain management for agri-food sector in Malaysia using blockchain technology,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 11, pp. 149–156, 2019.

[54] J. R. Wallrabenstein, “Practical and secure IoT device authentication using physical unclonable functions,” in *Proc. 2016 IEEE 4th Int. Conf. on Future Internet of Things and Cloud, FiCloud*, Vienna, Austria, pp. 99–106, 2016.

[55] A. S. Khan, “Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network,” *International Journal of Computer Networks and Communications*, vol. 6, no. 3, pp. 189, 2014.

[56] L. Hernández-álvarez, J. M. de Fuentes, L. González-Manzano and L. H. Encinas, “Privacy-preserving sensor-based continuous authentication and user profiling: A review,” *Sensors, Switzerland*, vol. 21, no. 1, pp. 1–23, 2021.

[57] Z. Ahmad, A. S. Khan, K. Nisar, I. Haider, R. Hassan *et al.,* “Anomaly detection using deep neural network for IoT architecture,” *Applied Sciences*, vol. 11, no. 15, pp. 1–19, 2021.

[58] S. Grooby, T. Dargahi and A. Dehghantanha, “A bibliometric analysis of authentication and access control in IoT devices,” In: Dehghantanha A., Choo KK. (eds.) *In Handbook of Big Data and IoT Security*, Springer, Denmark, pp. 25–51, 2019.

[59] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi and G. Srivastava, “Security aspects of internet of things aided smart grids: A bibliometric survey,” *Internet of Things*, vol. 14, pp. 100111–100145, 2019.

[60] A. Tandon, P. Kaur, M. Mäntymäki and A. Dhir, “Blockchain applications in management: A bibliometric analysis and literature review,” *Technological Forecasting and Social Change*, vol. 166, pp. 120649, 2021.

[61] Y. M. Guo, Z. L. Huang, J. Guo, X. R. Guo, H. Li *et al.,* “A bibliometric analysis and visualization of blockchain. *Future Generation Computer Systems*,” vol. 116, no. 1, pp. 316–332, 2021.

[62] D. Garg, J. Sidhu and S. Rani, “Emerging trends in cloud computing security: A bibliometric analyses,” *IET Software*, vol. 13, no. 3, pp. 223–231, 2019.

[63] S. R. T. Mat, M. F. A. Razak, M. N. M. Kahar, J. M. Arif and S. Mohamad, “Towards a systematic description of the field using bibliometric analysis: Malware evolution,” *Scientometrics*, vol. 126, pp. 2013–2055, 2021.

[64] P. Korom, “A bibliometric visualization of the economics and sociology of wealth inequality: A world apart?,” *Scientometrics*, vol. 118, no. 3, pp. 849–868, 2019.

[65] T. O. Olawumi and D. W. M. Chan, “A scientometric review of global research on sustainability and sustainable development,” *Journal of Cleaner Production*, vol. 183, pp. 231–250, 2018.

[66] A. S. Khan, S. U. Rehman, Y. K. Almaimouni, S. Ahmad, M. Khan *et al.,* “Bibliometric analysis of literature published on antibacterial dental adhesive from 1996–2020,” *Polymers*, vol. 12, no. 12, pp. 1–29, 2020.

[67] S. Ahmad, Y. Javed, S. H. Khahro and A. Shahid, “Research contribution of the oldest seat of higher learning in Pakistan: A bibliometric analysis of university of the Punjab,” *Publications*, vol. 8, no. 3, pp. 1–43, 2020.

[68] S. Ahmad, S. U. Rehman and M. Ashiq, “A bibliometric review of Arab world research from 1980–2020,” *Science & Technology Libraries*, vol. 40, pp. 1–21, 2021.

[69] M. Bastian, S. Heymann, M. Jacomy, “Gephi: an open source software for exploring and manipulating networks,” *in the Proc. of International AAAI Conference on Weblogs and Social Media*, California, USA, pp. 1–2, 2009.

[70] M. Koo, “Systemic lupus erythematosus research: A bibliometric analysis over a 50-year period,” *International Journal of Environmental Research and Public Health*, vol. 18, no. 13, pp. 1–14, 2021.