Analysis of Quantum Computing-Based security of Internet of Things(IoT) Environment

VARSHA ARYA[1], AMMAR ALMOMANI[2,3], CHUNJIA HAN[4],
[1]Asia University, Taiwan, Email: varshaarya21@gmail.com
[2]Research and Innovation Department, Skyline University College, P.O. Box 1797 - Sharjah, UAE
[3]IT-department- Al-Huson University College, Al-Balqa Applied University, P. O. Box 50, Irbid, Jordan, Email: ammarnav6@bau.edu.jo
[4]School of Business, Economics Informatics, Birkbeck, University of London, London, UK, Email: chunjia.han@bbk.ac.uk

ABSTRACT There is great potential in the Internet of Things (IoT) as an emerging technology. It can help us with a wide range of duties. On the one hand, the Internet of Things is a beneficial tool. However, on the other hand, it poses several significant security risks, such as data leaks, side-channel attacks, malware infections, and unauthorized access to data. Classical computers are well suited to classical cryptography techniques. Quantum computing, on the other hand, is on its way, and it has enormous processing power, making it possible to defeat present encryption techniques rapidly. Quantum computing, on the other hand, has the potential to undermine security ciphers. There is a need for new ways to protect against these risks. Using records of 15911 publications and their references in the Dimensions database, we construct a visual assessment of the quantum computing-based IoT security literature during the last decade. Current research and intellectual grounds reveal new trends in quantum computing and IoT application. It is possible to identify notable nations, organizations, and writers based on the volume of contributions in collaboration networks. In addition, the citation networks identify necessary studies and experts in the quantum computing-based IoT security literature, highlighting hot research and trends from 2011 to 2020. We also provide future recommendations in the field of quantum computing-based IoT security approaches. These findings are helpful for researchers and practitioners in the fields of quantum computing and the Internet of Things (IoT).

KEYWORDS Quantum computing, IoT, Security

I. INTRODUCTION

Internet of Things (IoT) refers to the vast interconnectedness of observable items with the capacity to communicate and do calculations, commonly referred to as the Internet of Things [1], [2]. Internet-based control and identification capabilities are also available. By 2025, the number of active Internet of Things (IoT) devices is expected to rise to 75 billion, according to some estimates [3]. Many diverse applications may be supported by the connectivity of all of these devices. This will help to automate processes, increase machine intelligence, and improve decision-making agility for a broad variety of industries [4], [5]. IoT equipment, such as wireless sensors, have limited computational and storage capacity, making managing large amounts of real-time data a major difficulty in many prospective IoT applications. Consequently, their more sophisticated processing duties are frequently performed on centralised servers or on the Internet's cloud [6]–[9]. As a security measure for IoT nodes, hash functions and cryptography are often used. For Internet communications, public-key cryptography's capacity to give high levels of security to websites, which was first made public in the 1970s [10]–[12], has made it an indispensable tool for those who use it. As a result, public-key cryptosystems are now included in a broad range of Internet protocols, including those used by regular computers as well as those found in the Internet of Things. If this is the case, then the suggested minimum key size should be increased. The National Security Agency (NSA) is supporting quantum-resistant options for storing sensitive information in light of the failure of the RSA key in 2010 [13], [14]. Therefore, developemnt of quantum computing based IoT security techniques are the hot research topic. Quantum computing-based IoT security technologies benefit from the detection of new patterns. To put it another way, it is important for researchers and practitioners to learn about developing trends and the underlying intellectual foundations of algorithms and protocols. It's also a plus if you can locate significant networks of collaboration and research towards quantum computing and IoT. Scholars and practitioners may use collaborative networks to find the best quantum computing and Internet of Things (IoT) research institutes. The most recent developments in quantum computing and the Internet of Things may be obtained by paying close attention to these institutions, and important studies will help provide a fundamental foundation for quantum computing-based IoT secrecy approaches, research hotposts, and trends.. The dynamics of quantum computing and the Internet of Things (IoT) have yet to be examined in a comprehensive examination [15], [16]. Using VOSviewer, we have collected 15911 records of research on quantum computing and IoT in the previous decade, which we then utilise to do a visual evaluation. Analysis of the phrases and keywords in these data reveals hot research and trends, and we uncover significant collaborations from networks of co-authors' networks.

II. DATA COLLECTION AND ANALYZING TOOLS

Our study relies on finding relevant publications and citation networks linked to quantum computing-based IoT security solutions in the scientific literature, which might reveal developing trends and collaboration networks in a subject. Researchers may search Dimensions database [17] for the most well-known academic publications as well as grant proposals, data sets, patents, and more. As a result, the Dimentions database is where we get our article entries and the related citation network. For the collection of relevent papers in the field of quantum compuitng that are based on IoT security from the Dimensions database, we use different search configuration to search the database “TS1=(“Quantum Computing" OR "Quantum Technology”)”, “TS2= (("Quantum Computing" OR "Quantum Technology") AND ("Internet of Things" OR "IoT" OR "IOT")”, and “TS3=(("Quantum Computing" OR "Quantum Technology") AND ("Internet of Things" OR "IoT" OR "IOT") AND (Security OR Privacy OR Secure)) ”. The time stpan for the data is selected as 2011-2020. After setting up the differnet quaries, we recived different papers as represented in Figure 1. As seen in Figure 1, quantum computing and quantum computing-based IoT security are burgeoning fields, as evidenced by the exponential growth in the number of publications over the previous decade. Therfoe, there is a need for a proper revire in this foeld that can guide the scholers about the recent trends the research problesm.

A. VOSVIEWER

For the purpose of creating and viewing bibliometric maps, we have relied on VOSviewer [18]. There are several uses for this application, including creating maps of authors or journals based on cocitation data, as well as creating keyword maps based on co-occurrence data. An in-depth perspective of bibliometric maps is provided by the software. Different methods of displaying a map in VOSviewer highlight distinct aspects of the map. It offers zooming, scrolling, and searching features that make it easy to examine a map in great detail. The VOSviewer's ability to display a huge number of elements makes it a great tool for large-scale maps. Our VOSviewer was the most recent release. The text mining features in VOSviewer have been much enhanced in this latest release. A corpus of documents may be used to create term maps as part of VOSviewer's text mining feature. Words are shown on a two-dimensional map such that the distance between any two terms may be used as an indicator of how closely the terms are linked. In general, the closer two words are, the more intimate their relationship. It is established by the number of times a term appears in a document that a term is connected.

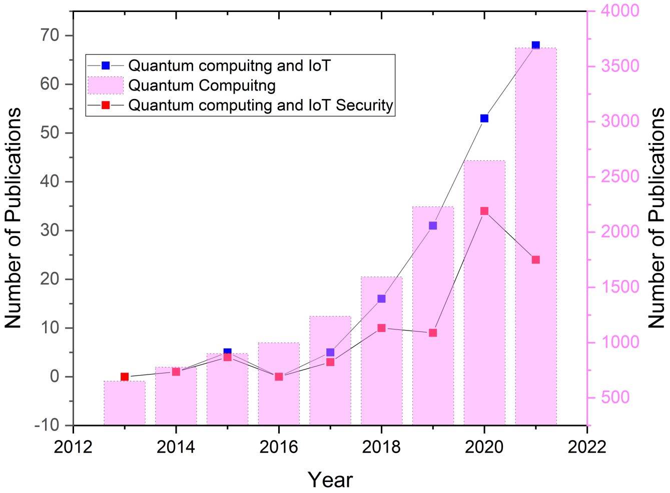

FIGURE 1: Total documents for Quaries TS1, TS2, and TS3

III. DATA ANALYZING OUTCOMES

Vosviewer has four functions: co-authorship, citation analysis, biblographic coupling, and co-citation analysis. Authors, institutions, and nations may be identified by co-authorship analysis. Co-occurring terms, such as the title, abstract, and keywords, might reveal research fronts and trends. Co-citation networks may be used to identify important studies, researchers, and journals in a certain topic.

A. LATEST RESEARCH AREAS

We analysed the abstracts and titles of the publications using VosViewer to identify keywords relevant to the research area. We find a total of 3574 relevant words from the abstract and title text, and then rank the 602 terms based on their frequency of occurrence. Additionally, we utilised the thesaurus file to tidy up the keyterms. The pattern of keyterms is shown in Picture 2, where the circle size denotes the phrase's frequency of occurrence; hence, if a term occurs often, it is represented by a larger circle in the figure. The colour of the circles is determined by the year of occurrence; for example, if a word occurs in 2021, it is marked yellow, and other colours are determined accordingly.

According to figure 2, researchers have been working in recent years in the fields of biomedical engineering, software engineering, image processing, computer vision, computer graphics, data assimanation, high performance computing, machine learning techniques, smart systems, smart agriculture, and image processing. Additionally, as seen in Figure 2, the biomedical keyword has the greatest linkage, indicating that the majority of researchers are working in this sector,

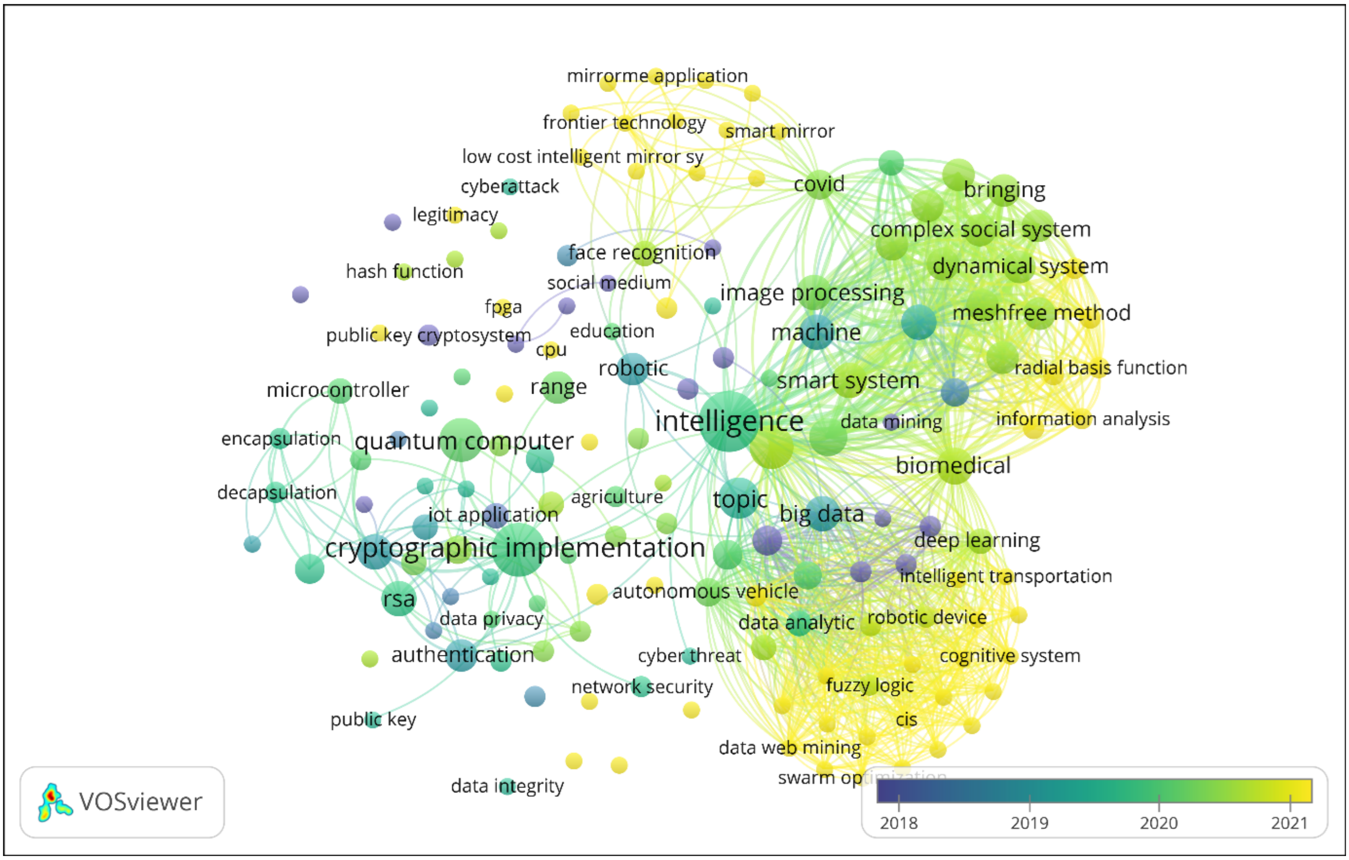

FIGURE 2: Most Appling reseah areas in the field of Quantun compuitng based IoT seurity

suggesting that it may be a good place to start for any researcher. To locate the region of research that is dry, we must seek for tiny circles with fewer connections in Figure 2. After thoroughly reviewing Figure 2, we can conclude that less work is being done in the fields of cyber attacks, hash functions, big quantum computers, public key encryptions, intelligent mirror systems, network security, and dark web, among others. As a result, researchers must concentrate their efforts on these areas in order to produce novel protocols and ideas that will improve the relevant profession.

B. COOPERATION NETWORK

It is possible to see how nations, institutions, and writers all interact together with VosViewer. This collaboration enables us to readily identify counties, institutions, and authors working in the subject of quantum computing-based IoT security. As seen in Figure 3, recognised nations collaborate closely on quantum computing-based IoT security. For the purpose of analysing inter-country cooperation, we use the threshold of two (Min, document published). In the recent decade, India and the United States have made the most significant contributions to quaintum computing-based IoT security. China, Egypt, Poland, the United Kingdom, South Korea, Taiwan, Saudi Arabia, Meixo, Canada, Luxembourg, Spain, Israil, Italy, and Bangladesh are the top followers in terms of frequency.

We set a threshold value of 2 as a starting point for discovering collaboration across different quantum computing-based IoT security research institutions throughout the globe (Min, number of documents publish). Due to the threshold value selection, 47 distinct clusters are produced based on the institutions' collaboration. The figure 4 illustrates the performance of several institutions in terms of collaborations, research output, and research quality in the area of quantum computing-based IoT security. From the network of institutions shown in Figure 4 and, we may identify institutions that have made significant contributions to the area of research. The circle's size indicates that the institution publishes more research articles than smaller circle institutes. The connection between the circles in Figure 4 denotes collaboration between the institutions. As illustrated in Figure 4, universities such as the University of Pune, the China Medical University, the Luxembourg Institute of Science, the Brono University of Technology, the Brandon University, the Dhaka International University, the Free University of Berlin, the Qatar University, and the University of Southern Queens are all working on quantum computing-based IoT security at the moment. Monterrey institute of technology collaborates with a large number of institutions, including nile university, jeddah university, menoufia university, and warsaw university. Following this, the China Medical Institute collaborates with

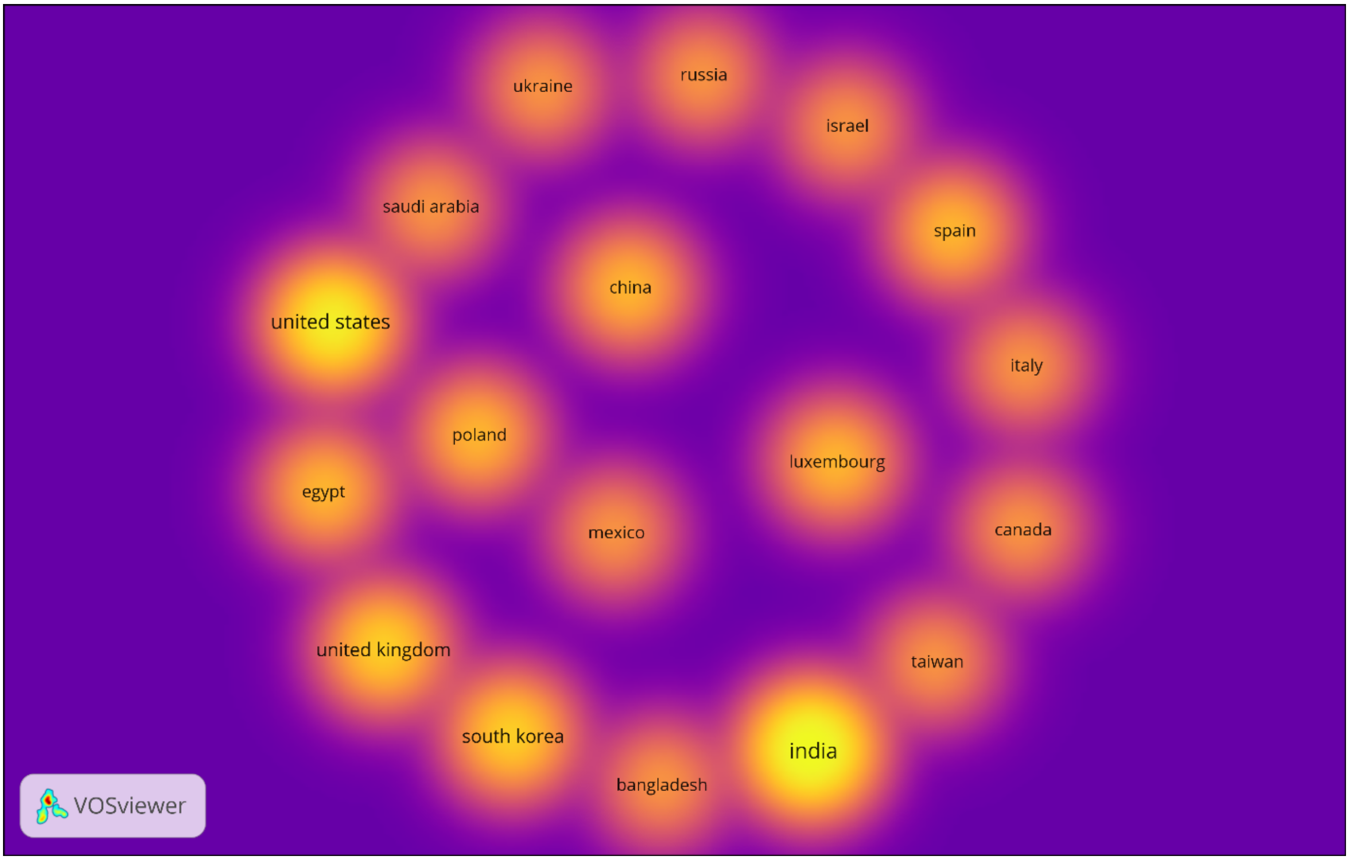

FIGURE 3: Country heat map

the largest number of institutions, including Qatat University, the University of Tartu, Brandon University, Brno University, and the University of Luxembourg. Thus, if a researcher want to collaborate on the development of novel molecules, he or she may contact one of these universities.

Co-authors play an important role in international networks of collaboration. During the last decade, we identified a portion of the co-author network in quantum comoputing based IoT security, as shown in Figure 5.

We have a total of 207 distinct writers in our database, which indicates that a significant number of authors are involved in the subject of quantum computing-based Internet of Things security. As soon as we've determined the number of writers, the next step is to determine the degree of collaboration between them. To do so, we set a threshold value of 2 (minimum number of documents) and created a collaboration map using VosViewer, which you can see below. Various clusters are shown in Figure 5 to illustrate the different parts of the map. According to the frequency of occurrence of coloboration, we obtain a total of 5 clusters. According to the figure 5, the authors, Uzzal Kumar, Parvz Gias Uddin, Mukta Ayesha Siddki, and Khandaker Mohammad Mohi Uddin are now working in collaboration on a project linked to quantum computing-based Internet of Things security, which is shown in the figure 5. Also included are the other writers, including abd-el-atty, bassem althobaiti, ohood saud, cheng chi, cheng hao, dohler mischa, el-latif ahmed a. abd, großschädl johann, mazurczyk wojciech, ryan peter y. a., rinne peter b., and venegas-andrac We may learn the names and contact information of the researchers who are the finest in the area of quantum computing and who are willing to share their expertise with others. As a result, any new researcher may benefit from the expertise of these researchers.

C. HIGHELY CITED PAPERS AND SOURCES

Any study is founded on research papers and publications in which relevant domains' research papers are published. If a high number of paers are available for a certain domain, it indicates that researchers are doing well in that discipline. Similarly to the research, the publishing source is critical to every research endeavour. As a result, we analyse the source of the publication in our study. According to our gathered data, there are a total of 59 worldwide publications where scholars publish their work on a regular basis. These journals are represented in figure 6, and their names are as follows: advanced sciences and technologies for security applications, advances in information security, advances in information security, privacy, and ethics, advances in intelligent systems and computing, aip conference proceedings, arxiv, communications in computer and information science, computer communications, computer science and information technology trends, digital communications

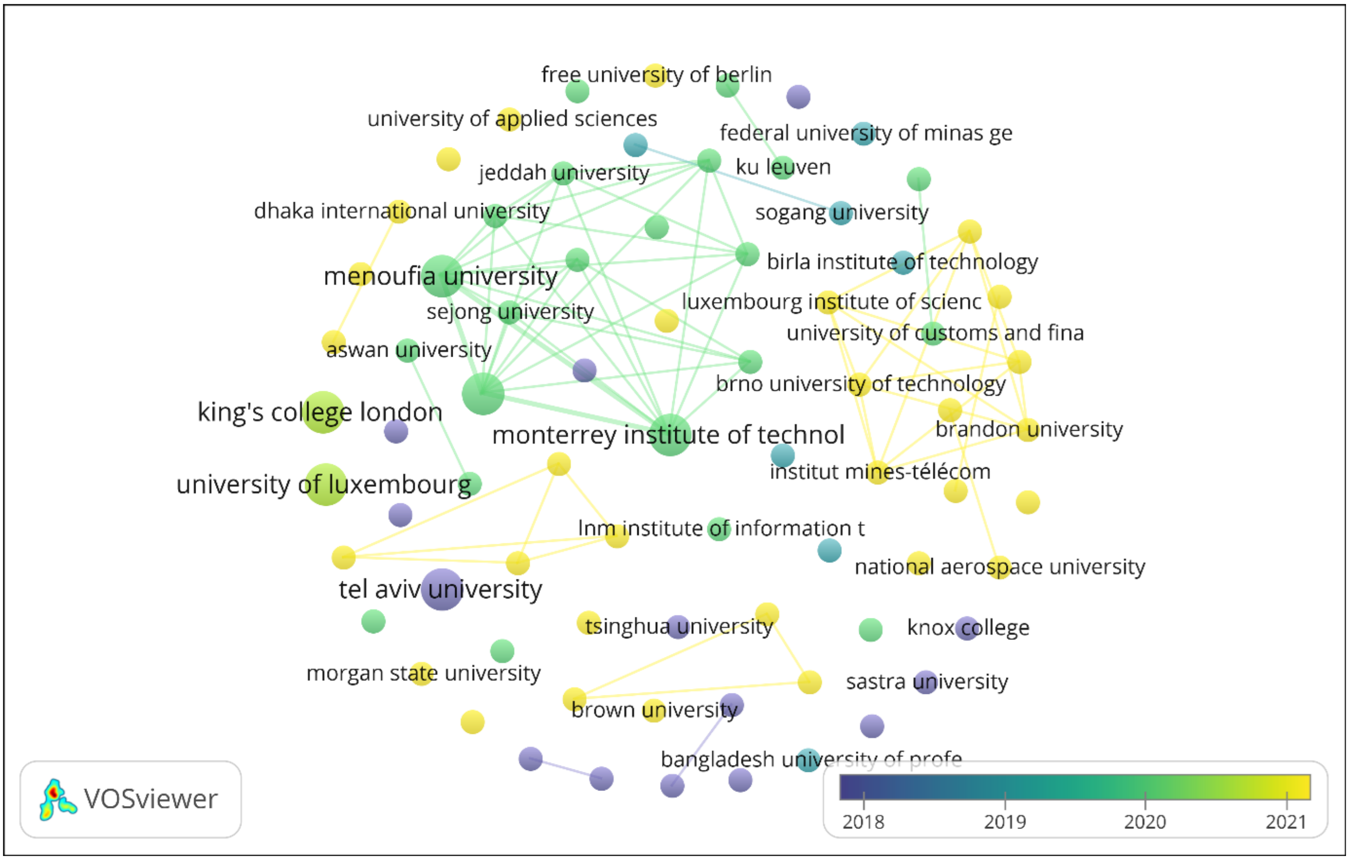
free university of berlin
university of applied sciences
federal university of minas ge
ku leuven
jeddah university
dhaka international university
sogang university
birla institute of technology
menoufia university
luxembourg institute of scienc
sejong university
university of customs and fina
aswan university
brno university of technology
king's college london
monterrey institute of technol
brandon university
institut mines-télécom
university of luxembourg
lnm institute of information t
national aerospace university
tel aviv university
tsinghua university
knox college
morgan state university
sastra university
brown university
bangladesh university of profe
VOSviewer
2018
2019
2020
2021

FIGURE 4: Institute Cooperation Map

and networks, e-management, electronics, entropy, foresight, handbook of multimedia information security: techniques and applications, health policy and technology, history of computing, iacr transactions on cryptographic hardware and embedded, systems, iacr transactions on symmetric cryptology, IEEE access, IEEE communications magazine, IEEE internet of things journal, IEEE transactions on network and service management, international journal of advances in soft computing and its applications, international journal of engineering and advanced technology, international journal of information technology, international journal of innovative technology and exploring engineering, international journal of research -granthaalayah, internet technology letters, it professional, journal of cybersecurity, lecture notes in computer science, lecture notes on data engineering and communications technologies, m/c journal, Mathematics, nato science for peace and security series b: physics and biophysics, proceedings of spie, quantum reports, revue d intelligence artificielle, science china information sciences, security and communication networks, sn computer science, ssrn electronic journal. From the figure 6 it is also clear that most of the papers of quantum compuitng based IoT securit are published in LNCS Springer and IEEE Access. Therfore, a new researchers can start their research by reading the current issues of these journals.

Selecting the appropriate research paper is also a critical step for every student, since the research paper contains detailed information about the issue. The number of citations indicates the validity and importance of the research article. Thus, in this section of the study, we outline the most referenced publications in the area of quantum computing-based IoT security. The breaf details of the five most cited papers are as follows:

- Cheng Ch et al. [19] have the most often referenced work (87 citations) in the subject of quantum computing-based IoT security. For IoT security, the authors concentrate on the present state of the art and new breakthroughs in the field of quantum-resistant cryptosystems. They first show how current cryptographic systems are vulnerable to assaults from both classical and quantum computers when using quantum computers, and then they offer an outline of the suggestions for future cryptographic schemes that can withstand these attacks as well. Next, authos demonstrates current IoT-compatible implementations of quantum-resistant encryption methods. Also included is an overview of current work on quantum-resistant techniques that will aid in the development of IoT security solutions in the future.
- The writers [20] from China have the second-highest number of citations (72 citations). The authors' goal

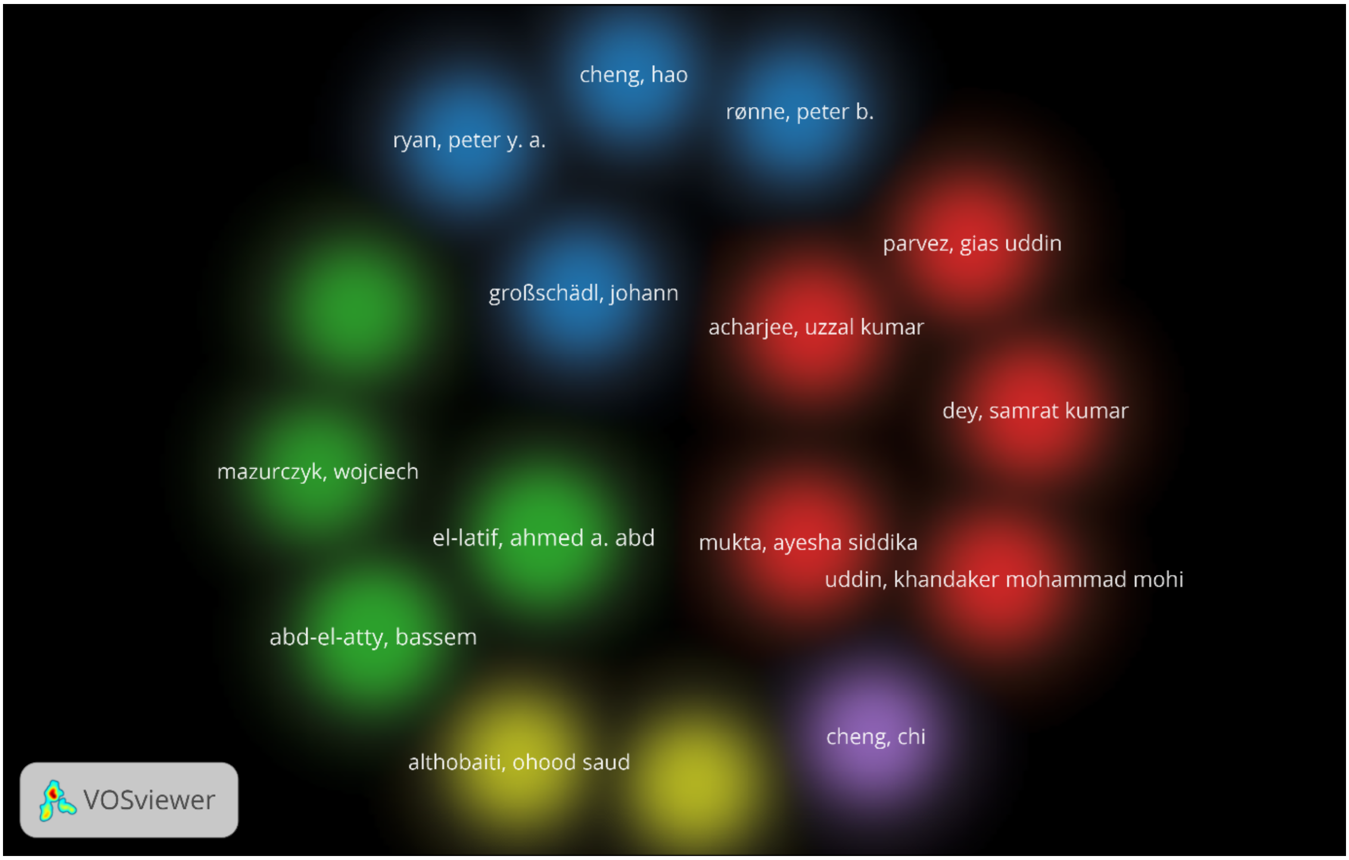

FIGURE 5: Author network analysis

is to investigate a new IoT scientific and technological foundation. In particular, a new cyber-physical-social-thinking environment is created by incorporating an intriguing notion of the Internet of Thinking, and a scientific and technical framework is then given that refers to both scientific and technological aspects. This framework of science and technology is explained in terms of traditional Chinese culture, which sees similarities between the "Five Elements" and IoT reformed cyber-physical science. Furthermore, they use a smart city scenario to identify the technological aspects of the Internet of Things and discuss the key enabling technologies. A new invention will be launched for academics and industry by the existing framework of science and technology.

- The author El-Latif, Ahmed A. Abd published two most cited papers in 2020 related to quantum computed. In the first paper [21] authors exploit the properties of quantum walk to develop a novel S-box approach which plays a vital role in block cypher algorithms for 5G-IoT technologies. As an application of the described S-box method and controlled alternative quantum walks for 5G-IoT technologies a new robust video encryption technique is offered. To create effective cryptographic methods based on quantum walks (QWs), you need a universal quantum computing model with intrinsic cryptographic properties. In As well as to satisfy demands of encryption for various data in 5G-IoT, we employ the properties of quantum walk to present an unique encryption approach for safe transmission of sensitive information in 5G-IoT paradigm. The primary purpose of the suggested cryptosystems is to store and communicate sensitive data across 5G networks in a safe manner, preventing unauthorised entities/objects from obtaining any relevant information about the sent data.." The analysis and findings of the suggested cryptosystems reveal that it has improved security features and effectiveness in terms of cryptographic performance. Authors in the second study [22] suggested a lightweight picture encryption technique based on quantum walks for secure data transport in IoT and WSN. Permutation boxes are constructed using the nonlinear dynamic behaviour of quantum walks, and pseudo-random numbers are generated by splitting the plain picture into blocks and then encrypting it. The provided encryption technique has been shown to be successful via simulation and numerical analysis. Analyzing the correlation of neighbouring pixels does not provide any helpful information about the ciphered picture since the encrypted images have randomness

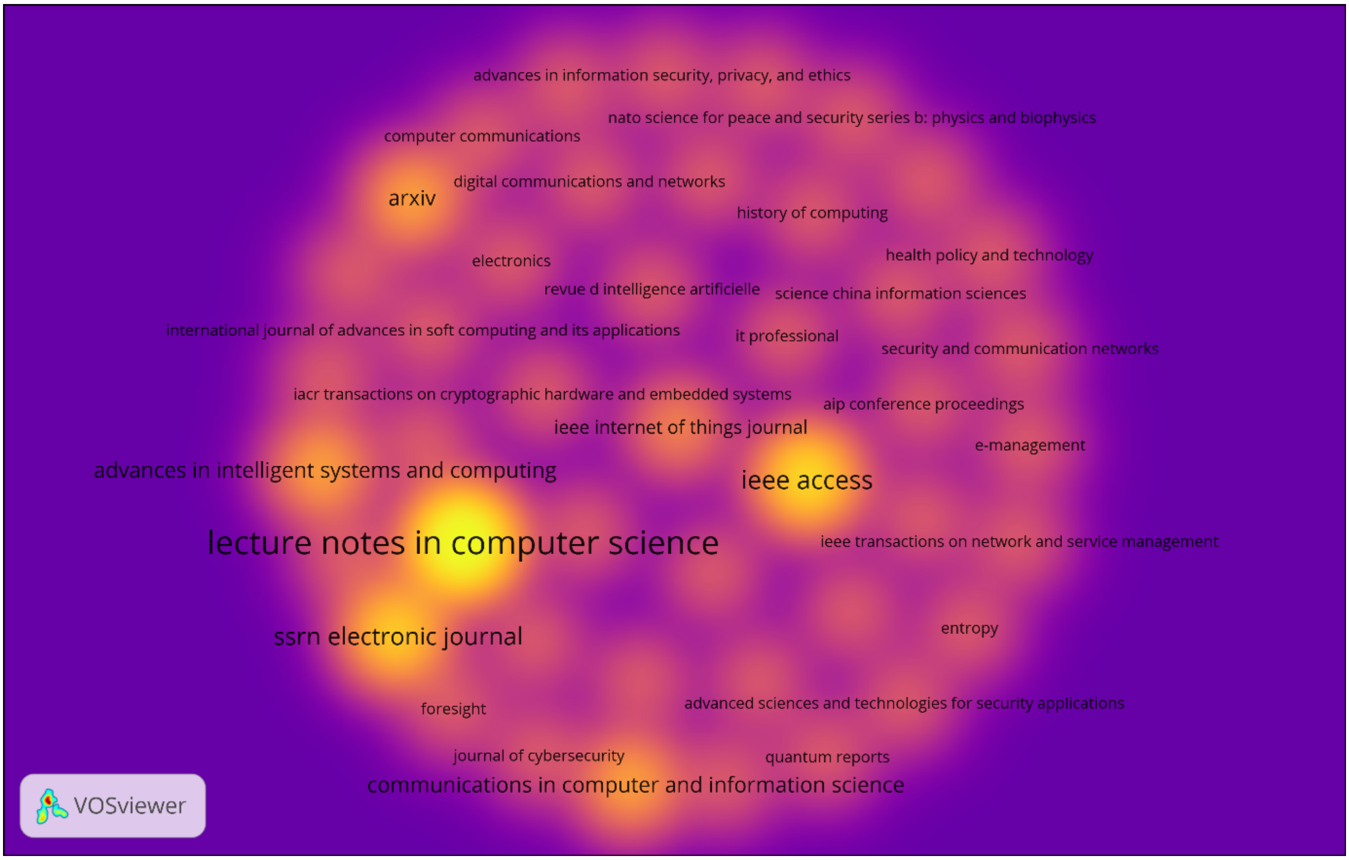

FIGURE 6: Analysis of Publication source

features. Furthermore, the key settings have a high level of sensitivity and a big key space to withstand a variety of assaults.

- Fernández-Caramés et al [13], prepared the most often referenced survey work on IoT security using quantum computing. IoT post-quantum cryptosystems and projects are examined in this article, as well as the most significant IoT designs and difficulties. Future developments are also predicted. Aiming to provide an overview of post-quantum IoT security, this study provides valuable advice for future post-quantum IoT designers.

IV. CONCLUSION

Our analysis of the quantum computing-based IoT security literature over the previous decade, using the Dimensions dataset and VOSviewer, revealed developing trends, collaboration networks, highly cited authors, and publishing sources, as detailed below. Quantum computers, quantum walks, cryptographic approaches, big data, autonomous cars, image processing, artificial intelligence, fuzzy logic, cooperative systems, swarm optimization, and cyber security are just a few of the latest study topics in which many academics are engaged. We must thus monitor these fields of study in order to assess the progress made in quantum computing. All major established and emerging countries, including the United States, China, India, and the United Kingdom, are pursuing quantum computing-based IoT security. Which results in the research area's overall development. All major research institutions in the aforementioned nations are also actively cooperating to create and improve the theories and protocols underlying quantum computing-based IoT security technologies. Well-known researchers working on quantum computing for IoT security include A.A. El-Latif, Mazurczyk Wojciech, Abd-El Atty Bassem, Cheng Chi, and Ning HuanSheng. These academics are establishing new ideas and notions that will aid future researchers in gaining an in-depth understanding of the study area. Additionally, leading journals such as LNCS spriger, IEEE access, IACR transection of cryptography, IEEE transection of network and service management, and SSRN electronic journals publish new researchers in the field of quantum computing-based IoT security, allowing researchers to stay current on the latest trends and developments in the field. Our conclusions are not based on all documents on quantum computing-based IoT security since we utilised a particular search option to retrieve information from the Dimensions database. It's possible that VOSviewer's algorithm may provide unexpected outcomes, such as assigning the same weight to all of the citations it finds to recognise notable studies and researchers. As a consequence, our findings are just an approximate reflection of the growth of the IoT security literature based on quantum computing. As a result, we'll be doing more study in the future that draws on several sources of data.

REFERENCES

[1] N. Kumar and et al., "A novel framework for risk assessment and resilience of critical infrastructure towards climate change," Technological Forecasting and Social Change, vol. 165, p. 120532, 2021.

[2] A. Tewari and et al., "Secure timestamp-based mutual authentication protocol for iot devices using rfid tags," International Journal on Semantic Web and Information Systems (IJSWIS), vol. 16, no. 3, pp. 20–34, 2020.

[3] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," Computer Science Review, vol. 31, pp. 51–71, 2019.

[4] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.

[5] M. Kaur and et al., "Secure and energy efficient-based e-health care framework for green internet of things," IEEE Transactions on Green Communications and Networking, vol. 5, no. 3, pp. 1223–1231, 2021.

[6] B. Joshi and et al., "A comparative study of privacy-preserving homomorphic encryption techniques in cloud computing," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–11, 2022.

[7] R. K. S. Rajput, D. Goyal, A. Pant, G. Sharma, V. Arya, and M. K. Rafsanjani, "Cloud data centre energy utilization estimation: Simulation and modelling with idr," International Journal of Cloud Applications and Computing (IJCAC), vol. 12, no. 1, pp. 1–16, 2022.

[8] B. B. Gupta, Modern Principles, Practices, and Algorithms for Cloud Security. IGI Global, 2019.

[9] B. B. Gupta, S. Yamaguchi, and D. P. Agrawal, "Advances in security and privacy of multimedia big data in mobile and cloud computing," Multimedia Tools and Applications, vol. 77, no. 7, pp. 9203–9208, 2018.

[10] C. P. Chen and C.-Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on big data," Information sciences, vol. 275, pp. 314–347, 2014.

[11] D. Singh, "Captcha improvement: Security from ddos attack," 2021.

[12] A. Gaurav, V. Arya, and D. Santaniello, "Analysis of machine learning based ddos attack detection techniques in software defined network," Cyber Security Insights Magazine (CSIM), vol. 1, no. 1, pp. 1–6, 2022.

[13] "The lens - free & open patent and scholarly search," https://www.lens.org/, accessed: 2023-01-01.

[14] S. R. Sahoo and et al., "Hybrid approach for detection of malicious profiles in twitter," Computers & Electrical Engineering, vol. 76, pp. 65–81, 2019.

[15] K. T. Chui and et al., "Enhancing electrocardiogram classification with multiple datasets and distant transfer learning," Bioengineering, vol. 9, no. 11, p. 683, 2022.

[16] ——, "Transfer learning-based multi-scale denoising convolutional neural network for prostate cancer detection," Cancers, vol. 14, no. 15, p. 3687, 2022.

[17] P. S. Emani, J. Warrell, A. Anticevic, S. Bekiranov, M. Gandal, M. J. McConnell, G. Sapiro, A. Aspuru-Guzik, J. T. Baker, M. Bastiani et al., "Quantum computing at the frontiers of biological sciences," Nature Methods, vol. 18, no. 7, pp. 701–709, 2021.

[18] P. Rebentrost, M. Mohseni, and S. Lloyd, "Quantum support vector machine for big data classification," Physical review letters, vol. 113, no. 13, p. 130503, 2014.

[19] M. Marghny, R. M. A. ElAziz, and A. I. Taloba, "Differential search algorithm-based parametric optimization of fuzzy generalized eigenvalue proximal support vector machine," arXiv preprint arXiv:1501.00728, 2015.

[20] D. Anguita, S. Ridella, F. Rivieccio, and R. Zunino, "Quantum optimization for training support vector machines," Neural Networks, vol. 16, no. 5-6, pp. 763–770, 2003.

[21] T. A. Shaikh and R. Ali, "Quantum computing in big data analytics: A survey," in 2016 IEEE international conference on computer and information technology (CIT). IEEE, 2016, pp. 112–115.

[22] R. Dridi and H. Alghassi, "Homology computation of large point clouds using quantum annealing," arXiv preprint arXiv:1512.09328, 2015.

.