3-3-2021

A Bibliometric Analysis of Authentication based Access Control in Cloud using Blockchain

Yogesh Gajmal
yogeshmgajmal@gmail.com

Udayakumar R.
rsukumar2007@gmail.com

A Bibliometric Analysis of Authentication based Access Control in Cloud using Blockchain

Yogesh M. Gajmal[1], R. Udayakumar[2]

[1]Research Scholar, Department of CSE, BIST, BIHER, Chennai, India, yogeshmgajmal@gmail.com

[2]Professor, School of Computing Sciences, BIST, BIHER, Chennai, India, rsukumar2007@gmail.com

Abstract:
Access Control is mentioned to as the imprisonment of particular activities of an individual to carry out an action. Cloud storing similar to any other untrusted surroundings wants the capacity to protect the shared data. The one of the apparatus of access mechanism is ciphertext-policy attribute-based encryption system over and done with dynamic characteristics. With a blockchain based distributed ledger, the scheme offers immutable log of whole significant safety events, for example key generation, change or revocation, access policy assignment, access request etc. Number of different problems similar to single point of failure, security and privacy etc. were targeted through the appropriate primary studies. The Meta analysis suggests the usage of diverse blockchain platforms, different application areas and different used blockchain properties. The services consist of authentication, privacy, confidentiality, data, access control list and, integrity assurance and resource provenance. Altogether these facilities are dangerous for the present distributed applications, particularly in line for to the huge quantity of information being processed over the webs and also the usage of cloud computing. Verification confirms that the client is who he/she professes to be. Confidentiality assures that the information cannot be read through unapproved users. Privacy gives to the clients the capacity to control who can get to their information. Provenance permits an effective tracing of the information also resources alongside using their ownership as well as utilization on the network. Integrity assists in authenticating that the information has not been changed or else altered. These services stand now managed through central controllers. On the other side, blockchain is a protected plus distributed ledger that can assist to resolve the issue of access control in cloud. We present a systematic analysis of blockchain driven access control systems. The current paper examines previous studies in the region of Access Control in Cloud, by a comprehensive Bibliometric study. The analysis is completed by using the Scopus databases also tools similar to Imap builder, VOSviewer and Word cloud. As of the database of Scopus, it is detected that the publications taking place Access Control in Cloud are 993 is Articles and 31 is a Review articles. The significant of research is limited but an increasing tendency is detected on or after the year 2013. The review shown that the maximum publications of Access Control in Cloud are journals articles and Conference Papers. Chinese top publications followed by the India and United States. The paper determines that the study area is recent also more research is obligatory in the domain Access Control in Cloud using Blockchain.

1. Introduction

Access Control, normally talk about to as resource approval or authorization, is the imprisonment of the activities of a specific an individual only towards the work out resources as well as services that it is legal to usage. This is completed through applying predefined access control rules. The fundamental rules govern each access of an individual to a specific resource. The rules can be acknowledged in the appearance of properties and the comparing rules related with a bunch of entities and a bunch of assets. For the access mechanism to be sound as well as make sure integrity, this is accomplished by securely starting the uniqueness of the entities. If this safety implementation of the formation of identities is absent, applying an access rule is thwarted and left unusable. Even though there is an absolute as well as terrible necessity to apply access control mechanisms in preparation, it starts with problems that need careful thought before these mechanisms are put to execution. Several of the challenges are; it is challenging to attain access control in assets forced devices in line for to their varied nature as well as limited computation abilities. Similarly, the changeable nature of devices creates it tough towards implement access control rules. Additional significant features that are stimulating are the changeable topologies, diverse nature, also rule enforcement dynamically. Although all of this originates down to whether an answer is feasible, captivating into thought considerations like time-memory tradeoffs, behavior to diverse types of traffic, resistance in contrast to different attacks, in addition to adaptability to dynamic variations to the network are supreme. Nevertheless, these problems can be share out with abundant comfort if a diverse viewpoint is put in place.

In the previous some years, facilities to remotely storing and synchronize client information on cloud-based facilities have been augmented. So, many users are storing their files/documents in the clouds. However, there are certain safety glitches. The vital issue is moving information to the outside surroundings, such that anybody else other than the holder can get access to data.
On the other side, it is challenging to provide in to the many services that offer facilities used for information storing: backup documents, the capability to access their files from any device from anyplace in the world, simply transmission of documents to another user. You can discover some techniques to resolve the issue of safe remote file storing. Nonetheless the furthermost effective of them is to encode information before transfer. Encoding is one of the key defensive mechanisms suggested through the Cloud Safety Association. On the other hand, encoding carry out certain trouble to usage the information as well as the shared access to them.

Currently, A Blockchain is a protected, shared also dispersed ledger that simplifies the procedure of record as well as tracking resources deprived the necessity of a central trusted specialist. It permits two parties to interconnect also interchange resources into a network wherever dispersed

decisions are complete through the majority rather than by a single central specialist. It is provably protected in contradiction of attackers who attempt to regulate the scheme by compromising the central control. Assets can be tangible or else intangible. In common, whatever that has a worth can be followed on a blockchain to decrease its safety problems also save the charge of safety observing for all included.

In recent times, the blockchain skill has involved marvelous attention from academia as well as industry. The skill presently spans numerous applications that are widely held as well as motivating the networking investigation. Applications consist of healthcare, Internet of Things, also cloud storage. Normally, the blockchain has established its potential in several applications that now needs a central record. Amongst the blockchain promising applications are network monitoring as well as safety services together with authentication, privacy, confidentiality, provenance, also integrity. At present, these facilities are providing through trustworthy third-party agents otherwise with incompetent dispersed methodologies. Because of this, safety is a main challenge for present applications. On the other side, the blockchain technology can offer safety assurances that solve several old-style challenges in adding to providing a completely distributed, provably safe, also consensus solution. Fig. 1 shows the dissimilarities amongst the old-style and the blockchain-based access mechanism.
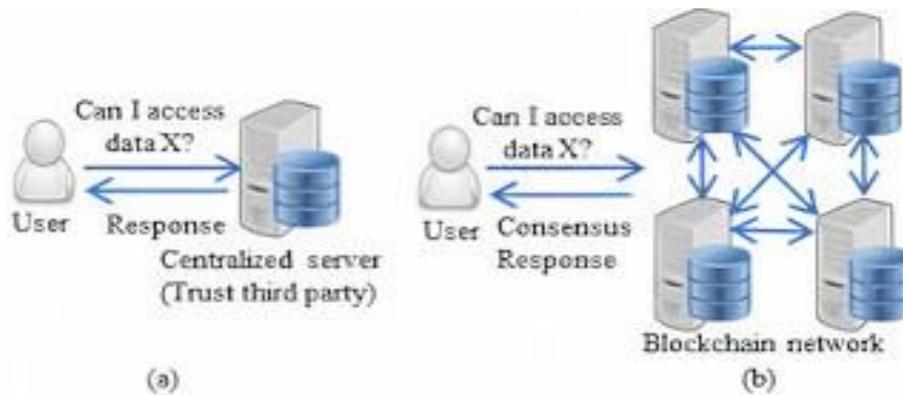

Fig. 1 (a) Traditional centralized access control (b) Blockchain based access control

The tenacious problems with old-style access mechanisms are considered in this opinion, also it is obvious from the current works that blockchain technology certainly has supremacy over it.

[J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander.] In their conclusions, they disclose the most of the papers attentive on Bitcoin projects, in detail below a common theme tune of safety and secrecy. This review providing a moving stone for the equivalent research community to see the sights in this path further.

[Sara Rouhani and Ralph Deters] have showed a state of the art review taking place on blockchain-based access control schemes also challenges. In specific, they have highlighted the

difficulties come across by the present access control schemes as well as how blockchain can be used to solve such difficulties.

[F. Casino, T. K. Dasaklis and C. Patsakis] had shown a comprehensive systematic analysis of Blockchain applications. In specific, they gives a arrangement of Blockchain-based applications across different domains reaching on or after supply chains to IoT, and they similarly highlighted obstacles in Blockchain technology, which bound the mass usage of Blockchain technology. Nevertheless, very limited articles in the literature have showed a review on Blockchain application in access control.

This Bibliometric analysis is intended to review the study contributions in the area on Access Control in Cloud using Blockchain and its allied areas over the period of last 10 years. This study gives comprehensive statistics about worldwide research and is categorized country wise, source wise, area wise etc. also will help as path discoverer for the research candidates in the area of Access Control in Cloud using Blockchain with essential understandings for forthcoming work.

2. PRIMARY DATA COLLECTION

Intended for this Bibliometric analysis we have well thought-out Scopus database which is major database of peer studied literature which provides the whole understandings to scientific global research in diverse arenas. The keywords used to exploration the database are shown below.

Table 1: Keywords used for studying Scopus Database

Master Keywords	"Cloud Computing" AND "Access Control" AND "Blockchain"
Primary Keywords	"Authentication" OR "Privacy" OR "Data Sharing" OR "Encryption" OR "Security" OR "Cloud Storage System" OR "Data Retrieval"

"Cloud Computing" AND "Access Control" AND "Blockchain" are used as master keywords for penetrating through the database which outcomes with about 20,000 plus publications nonetheless it has been filtered to 2381 search outcomes by with few main keywords (Data access till Feb. 22nd, 2021). Figure 1 displays the word cloud of the whole thing keywords considered intended for doing this Bibliometric analysis.

The cluster analysis of authors through the publication of past 10 years is completed via "VOSviewer" software tool. Figure 2 shows the cluster analysis of authors as underneath. One can simply focus the development of research in the Access control associated areas over the period of previous 10 years via cluster analysis.

Figure 1: Word Cloud of Keywords (Data access till Feb. 22nd, 2021)

Figure 2: Cluster Analysis of Authors (Data access till Feb. 22nd, 2021)

3. DATA ANALYSIS AND INTERPRETATION

As per the Scopus database is the maximum popular scientific database; the information collected as of there to carry out literature analysis with diverse concerns like affiliation,

publication year, subject area country wise, authors, access type etc. and it is showed in this section.

3.1 Analysis by Affiliation, Author, and Language of Publication

As per the information collected; Xidian University, China is at the helm with 106 publications followed by Chinese Academy of Sciences, China with 55 publications among top 10 affiliations that are well thought-out for this study. A total of 473 publications are renowned for the topmost 10 affiliations in the present study of Bibliometric analysis.
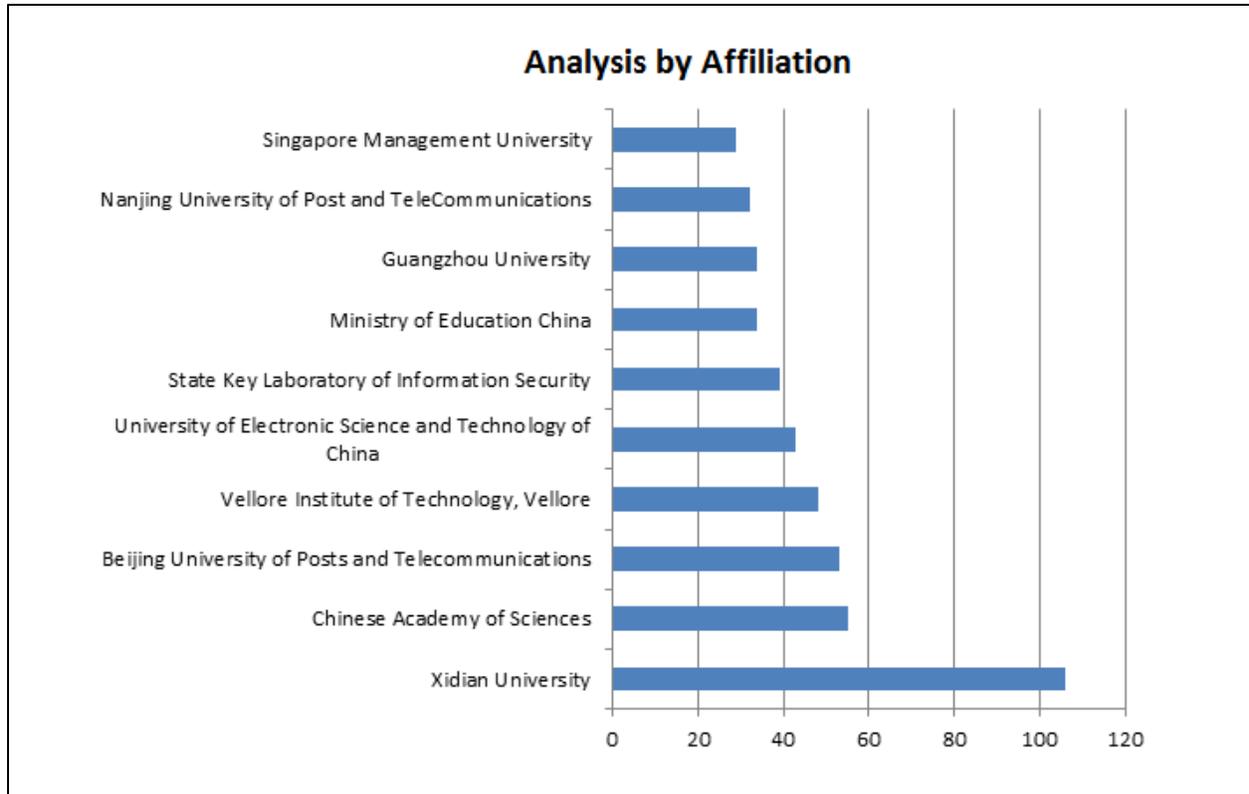

Figure 3: Analysis by Affiliation (Data access till Feb. 22nd, 2021)

As showed in Figure 4, a total of 191 research articles are published through topmost 11 worldwide authors. As far as the mentioned data; furthermost of the authors having affiliation through Xidian University, Chinese Academy of Sciences and Beijing University of Posts and Telecommunications while from India, Vellore Institute of Technology, Vellore and Anna University are in top affiliations.
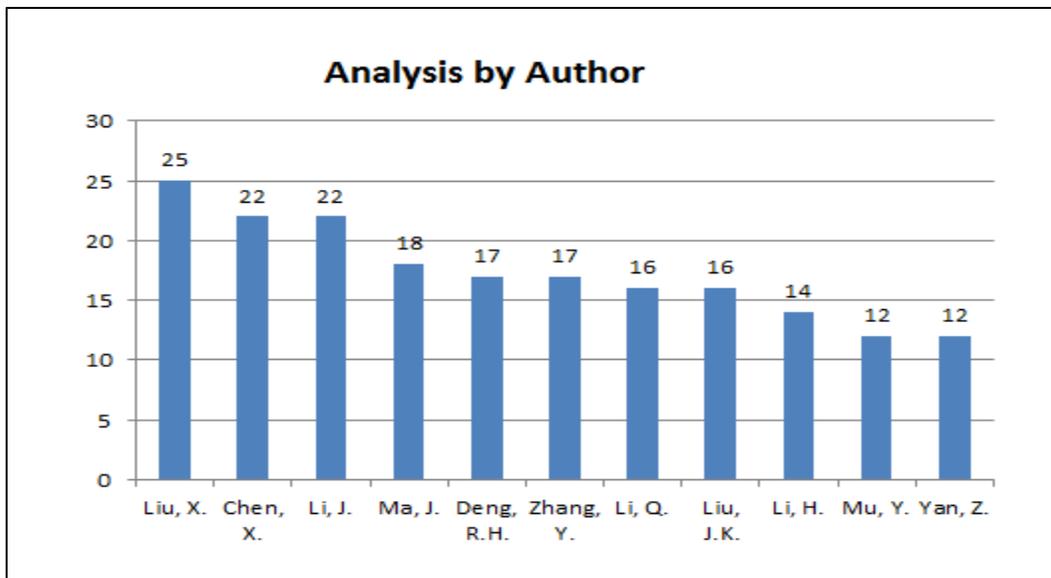
Figure 4: Analysis by Author (Data access till Feb. 22nd, 2021)

Regarding the language of publication; a total of 2314 articles are published in an English language while other languages like Chinese and German are having 77 and 1 respectively. More than 90% of research work is published in English language to have a global scope.

Table 2: Language wise Publication details

Sr. No.	Publication Language	No. of Publications in Scopus
1	English	2314
2	Chinese	77
3	German	1

3.2 Analysis by Access and Document Type

This type of analysis is used to classify diverse articles depend on their access type as well as the document type. Talk about the selection of data for this specific analysis, the more number of research articles are open access also rest are classified into diverse categories wiz Gold, Hybrid Gold, Bronze and Green. As shown in Figure 5, a total of 468 articles are open access shadowed by Green category consisting of 231 articles.
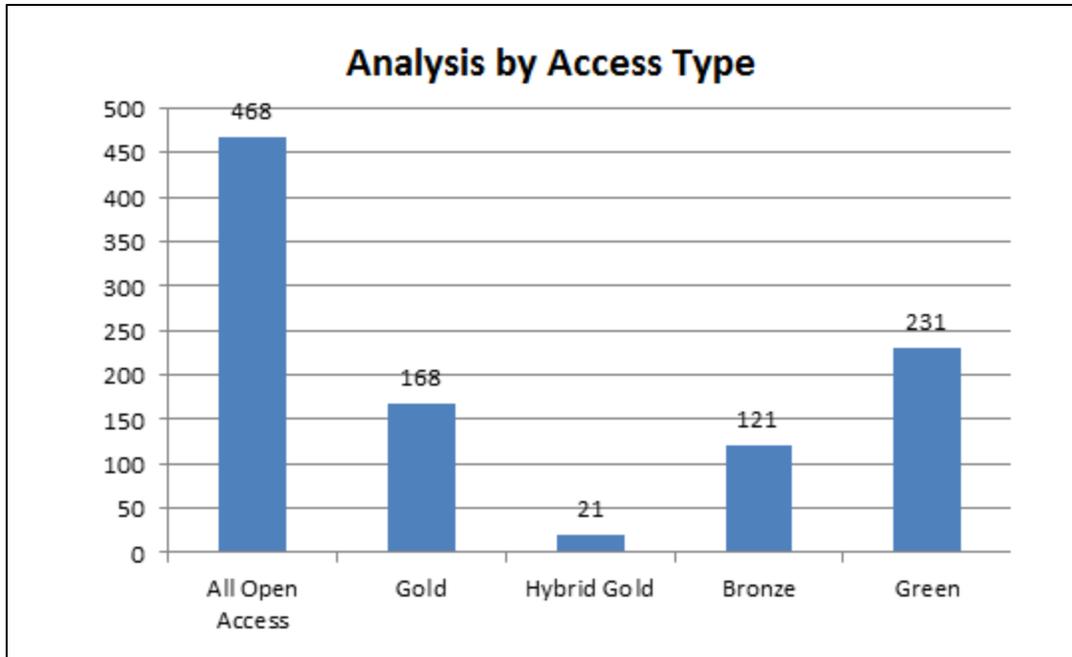
Figure 5: Analysis by Access Type (Data access till Feb. 22nd, 2021)

Table 3: Summary of Data based on Document Type (Data access till Feb. 22nd, 2021)

Sr. No.	Document Type	No. of Publications in Scopus
1	Conference Paper	1190
2	Article	993
3	Conference Review	105
4	Book Chapter	60
5	Review	31
6	Book	2

Table 3 display the summary of information collected for this review. It clearly shows that the more numbers of publications are into the form of Conference papers followed by research articles. Few of the publications are also made as a part of Conference Review, book chapters etc.
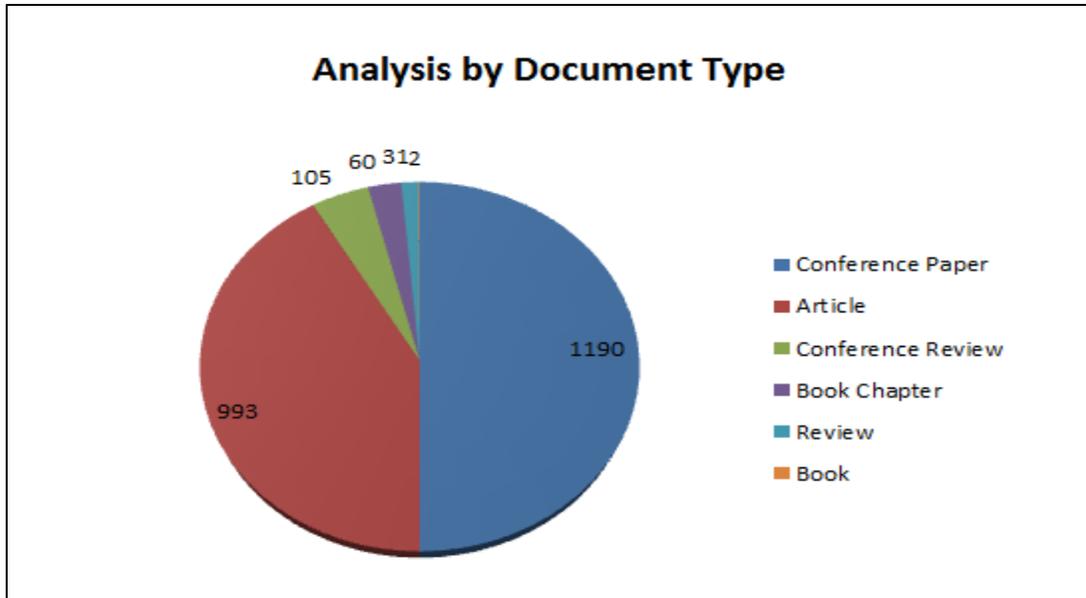
Figure 6: Analysis by Document Type (Data access till Feb. 22nd, 2021)

3.3 Analysis by Year

In this segment, the specific summary of publications completed on year to year basis is signified with a complete study. The publications from 2010 to 2021, i.e. past 12 years are considered for current study. The study displays that the more numbers of publications are completed in the year 2018 creation the threshold of 338 publications, which was the maximum in previous 12 years. By seeing Figure 7, it is obvious that the research tendency in Access Control in Cloud using Blockchain is rising significantly. Given the modern growth in the arena of Access Control, it is predicted that the next era will be of intelligent objects interactive as well as exchanging data to create life relaxed for human being.
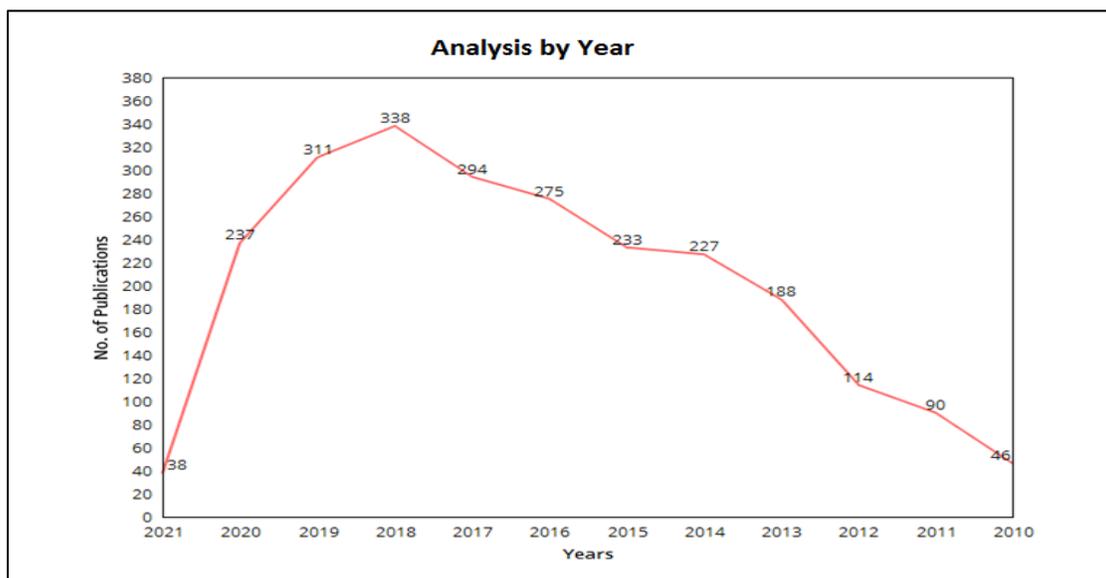
3.4 Analysis by Subject Area

The subject area analysis contributions in knowing key attentiveness areas for the current study. As presented in Figure 8, a highest 2021 publications are completed in the area of Computer Science shadowed by 876 in the Engineering area. The maximum input is recognized in Computer Science areas are permitted to Access control in cloud. A lot of research work is ongoing in this area refer to advance these Access controls

Noteworthy contributions are also renowned in the area of Mathematics, Physics and Astronomy as well as Decision Sciences. By seeing the analysis tendencies, it seems that the contributions are made into diverse areas by creating union of them to create Access control in cloud truly interdisciplinary research area. In spite of this, areas similar to Agricultural and Biological Sciences, Biochemistry, Genetics and Molecular Biology, Chemical Engineering, Pharmacology, Toxicology and Pharmaceutics can be taken ahead in coming days.
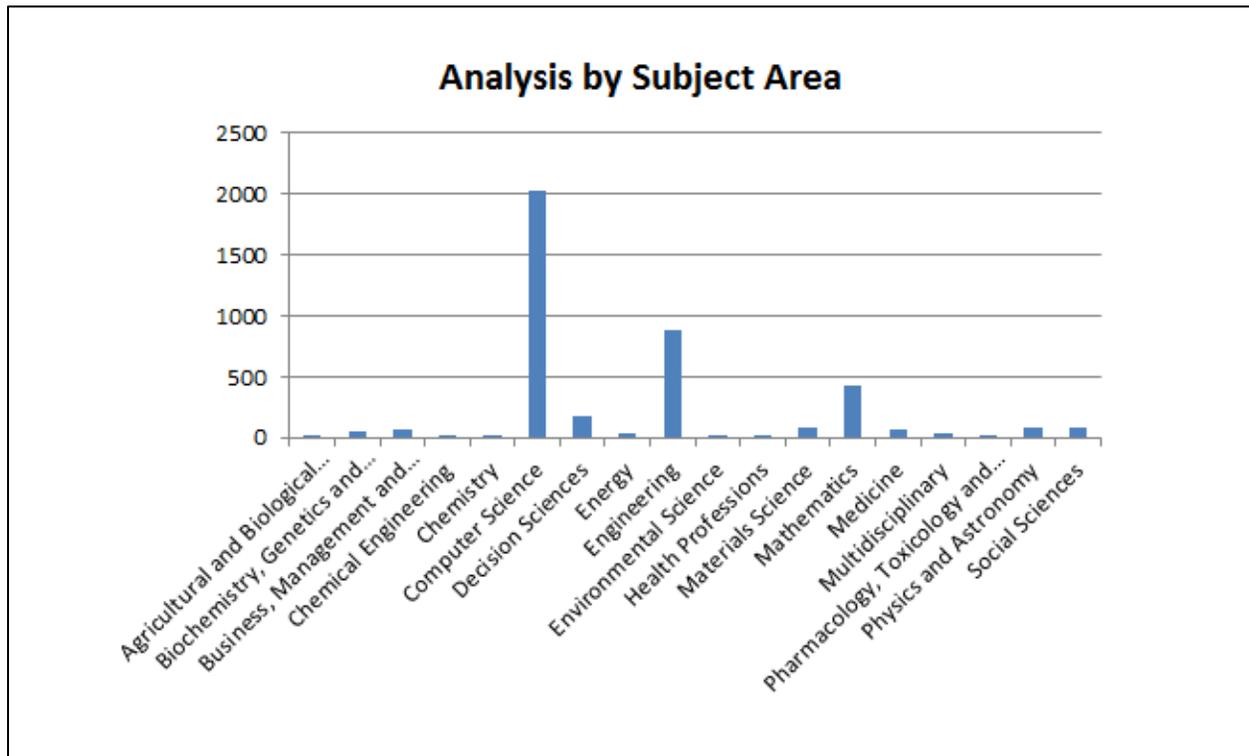

Figure 8: Analysis by Subject Area (Data access till Feb. 22nd, 2021)

3.5 Analysis by Source

This section précises around the research contributions completed from diverse sources of publications recognized with the assistance of Scopus database. A highest 132 publications are noted as of the Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics, followed by 57 in the IEEE Access.

Further down Table 4 displays the immediate summary of data concerning the analysis from topmost 12 sources. Figure 9 shown the study based on source for the Scopus database in analysis.

Table 4: Summary of Data based on Source (Data access till Feb. 22nd, 2021)

| Sr. No.	Source Title	No. of Publications in Scopus
1	Lecture Notes In Computer Science Including Subseries Lecture Notes In Artificial Intelligence And Lecture Notes In Bioinformatics	132
2	IEEE Access	57
3	ACM International Conference Proceeding Series	42
4	Communications In Computer And Information Science	41
5	Advances In Intelligent Systems And Computing	38
6	Future Generation Computer Systems	33
7	International Journal Of Applied Engineering Research	26
8	IEEE Transactions On Cloud Computing	21
9	Lecture Notes In Electrical Engineering	21
10	IEEE International Conference On Cloud Computing Cloud	19
11	Journal Of Advanced Research In Dynamical And Control Systems	19
12	IEEE Transactions On Dependable And Secure Computing	18
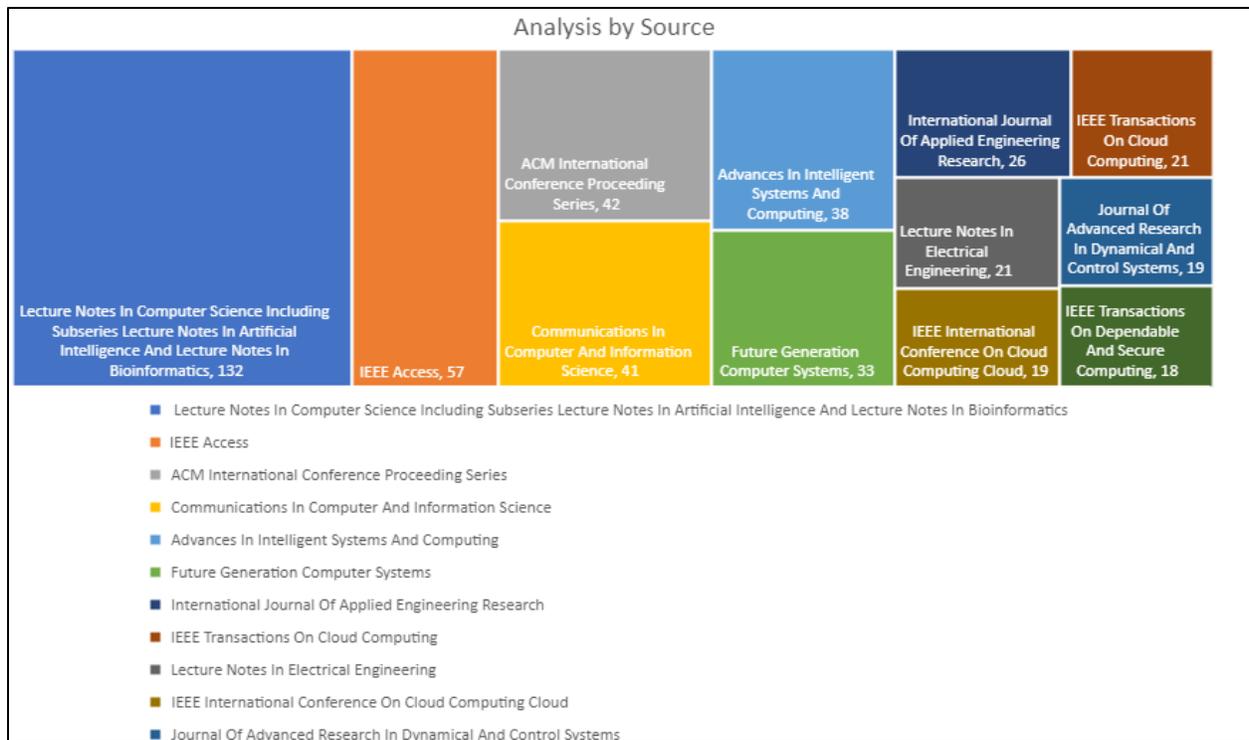
Figure 9: Analysis by Source (Data access till Feb. 22nd, 2021)

3.6 Analysis by Country

Nation wise analysis is obtainable to understand the deliberations in the original research area. Based on the designated Scopus database above the period of previous 12 years, it is obvious that china is a frontrunner in Access Control related research contributions with a highest 810 publications.
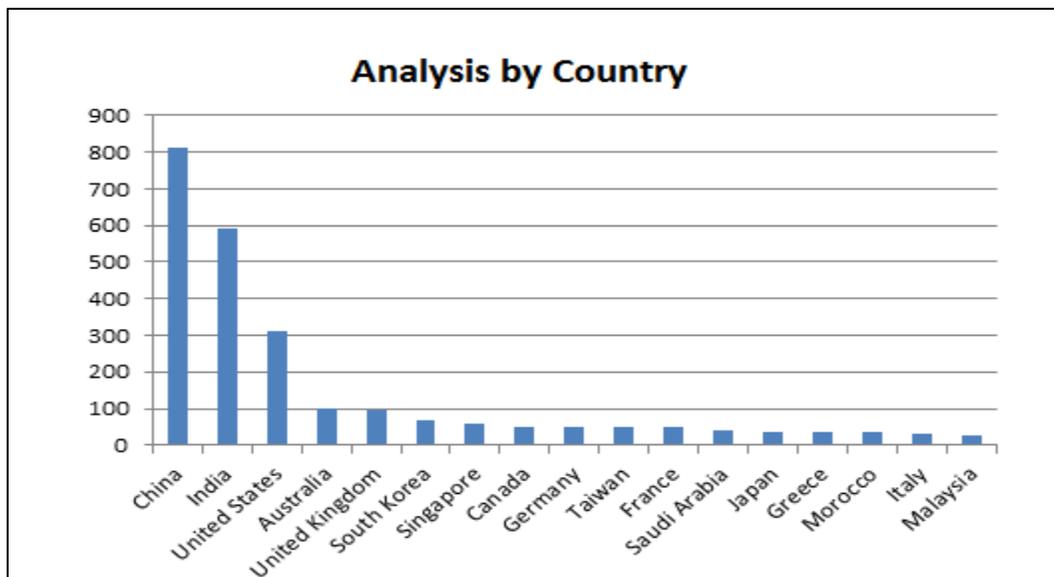

Figure 10: Analysis by Country (Data access till Feb. 22nd, 2021)

India, United States, Australia and United Kingdom are as well made noteworthy contributions in research publications in this area. Figure 10 exemplifies the nation wise analysis based on the Scopus database in consideration. The top 17 countries are in use into account to signify this study. Adding to this, geographical locations map showing countries contributing to publications in the worried area is showed in Figure 11. The further down map is ready using Imap builder software also can visibly denote the universal growth in Access Control associated research contributions.
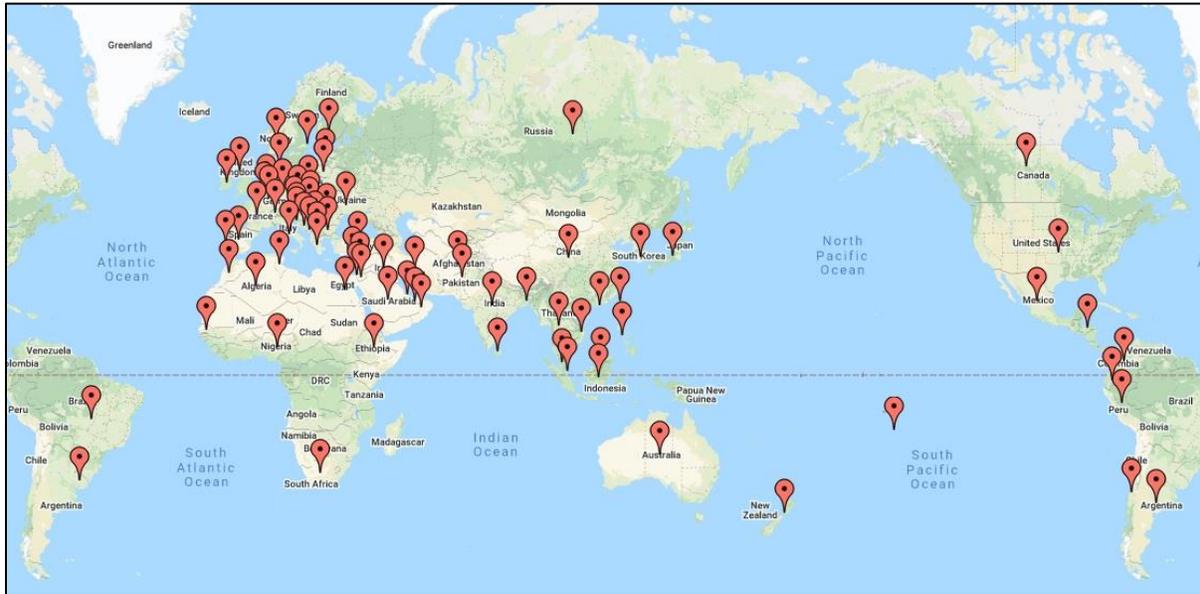

Figure 11: Topographical Locations of the Country (Data access till Feb. 22nd, 2021)

3.7 Analysis by Funding Sponsor

This section emphases of the funding analysis as research backing is serious for any research effort also it helps the aids in the concerned area by extremely inspired as well as attentive researchers. It acts as substances to increase up the research procedure also in current time many funding organizations have come frontward in this regard to encourage research as well as innovation. Figure 12 represents the analysis for the top 13 funding sponsors universal in the concerned study area.

Table 5: Summary of Data based on Funding Sponsor (Data access till Feb. 22nd, 2021)

Sr. No.	Source Title	No. of Publications in Scopus
1	National Natural Science Foundation of China	324
2	Fundamental Research Funds for the Central Universities	55
3	National Basic Research Program of China (973 Program)	54

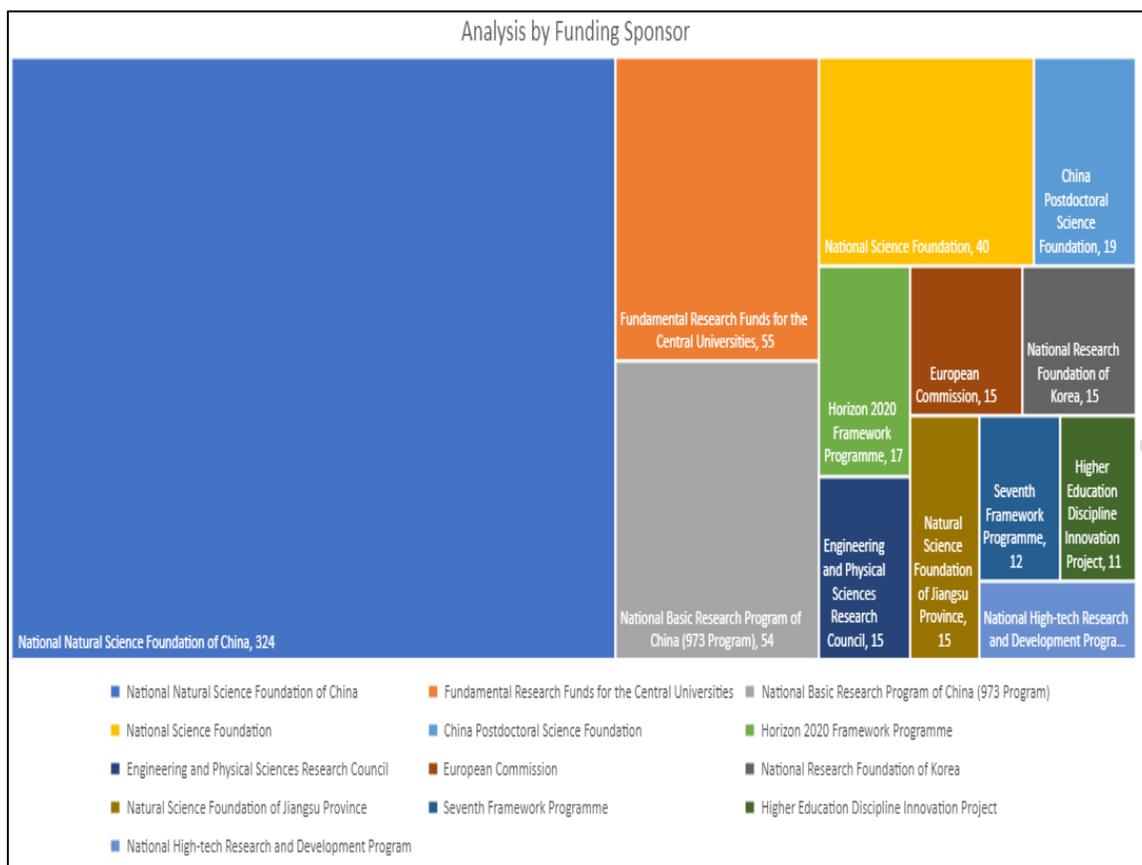| 4	National Science Foundation	40
5	China Postdoctoral Science Foundation	19
6	Horizon 2020 Framework Programme	17
7	Engineering and Physical Sciences Research Council	15
8	European Commission	15
9	National Research Foundation of Korea	15
10	Natural Science Foundation of Jiangsu Province	15
11	Seventh Framework Programme	12
12	Higher Education Discipline Innovation Project	11
13	National High-tech Research and Development Program	11

Figure 12: Analysis by Funding Sponsor (Data access till Feb. 22nd, 2021)

As stated in Table 5, National Natural Science Foundation, China is the top funding agency contributing with 324 publications followed by National Basic Research Program of China. Figure 12 signifies analysis through funding sponsor based on information collected as of Scopus database for this Bibliometric analysis.

Conclusion:

In this article, we presented a comprehensive analysis on the utilization of the blockchain in access control. Access control has demonstrated on numerous occasions to be a similarly significant security highlight like some other component in each security framework. Surely, there are defects with the old-style access control schemes; also efforts are placed to beat the issues consistently. Still, after the beginning of blockchain technology, access control schemes have started to make a diverse road-map of fundamental as well as forthcoming challenges to tackle. This paper presenting the Bibliometric analysis completed with Scopus database, to make available an overview of the hard work completed by the researchers in the area of Access Control in cloud using Blockchain. The current study specifies that the previous researches are mainly in the area of Role based access control, Attribute based access control, fine-grained access control etc. The numbers of publications are show an increasing tendency from 2012, representing the research area is forthcoming. This analysis discloses that maximum of the articles on Access Control in cloud are available in the English language also the key contributors to the research are China, India, United States, Australia and United Kingdom. It is detected that most research funding in this area is provided by National Natural Science Foundation of China. The studied literature recommends that, even though problematic awareness is tall, extra research is required to make extra dominant, immediate as well as global clarifications to advance the present participations to bounds the amount of Access Control in Cloud. The entire numbers of publications in Scopus are some degree of indicating necessity of additional research in the area of Access Control in Cloud using Blockchain.

REFERENCES

[1] Aaqib Dar & Auqib Lone(2021). Blockchain Driven Access Control Mechanisms, Models and Frameworks: A Systematic Literature Review. Elsevier, January 27, 2021

[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander (2016), Where is current research on blockchain technology?|a systematic review, PloS one 11 (10) e0163477.

[3] F. Casino, T. K. Dasaklis, C. Patsakis (2019), A systematic literature review of blockchain-based applications: current status, classi_cation and open issues, Telematics and Informatics 36 55-81.

[4] S. Rouhani, R. Deters (2019), Blockchain based access control systems: State of the art and challenges, in: IEEE/WIC/ACM International Conference on Web Intelligence, pp. 423-428.

[5] B. Bera, D. Chattaraj, and A. K. Das (2020). Designing secure blockchain based access control scheme in iot-enabled internet of drones deployment. Computer Communications, 153:229-249.

[6] H. Liu, D. Han, and D. Li (2020) Fabric-iot: A blockchain-based access control system in iot. IEEE Access, 8:18207-18218.

[7] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu (2020). Fadb: A fine grained access control scheme for vanet data based on blockchain. IEEE Access, 8:85190-85203,.

[8] H. Xu, Q. He, X. Li, B. Jiang, and K. Qin(2020). Bdss-fa: A blockchain-based data security sharing platform with fine-grained access control. IEEE Access, 8:87552-87561.

[9] Ilya Sukhodolskiy & Sergey Zapechnikov (2018). A Blockchain Based Access Control System for Cloud Storage. IEEE, 1574-1578

[10] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander (2016), Where is current research on blockchain technology?|a systematic review, PloS one 11 (10) e0163477.

[11] Sukhodolskiy I. A., Zapechnikov S. V.(2017) An access control model for cloud storage using attribute-based encryption. In Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE Conference of Russian (pp. 578-581).

[12] Horvath M. (2015) Attribute-Based Encryption Optimized for Cloud Computing. In SOFSEM 2015, LNCS 8939, pp. 566-577.

[13] Tara Salman & Maede Zolanvari (2019). Security Services Using Blockchains: A State of the Art Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019

[14] M. Pilkington{2018) , "Blockchain technology: Principles and applications," in Research Handbook on Digital Transformations. Cheltenham, U.K.: Edward Elgar, 2016. Accessed: Feb. 13, 2018. [Online]. Available: https://ssrn.com/abstract=2662660

[15] M. Mettler (2016), "Blockchain technology in healthcare: The revolution starts here," in Proc. IEEE 18th Int. Conf. e-Health Netw. Appl. Services (Healthcom), Munich, Germany, 2016, pp. 1–3.

[16] M. E. Peck (2017), "Blockchain world—Do you need a blockchain? This chart will tell you if the technology can solve your problem," IEEE Spectr., vol. 54, no. 10, pp. 38–60, Oct. 2017.

[17] G. Zyskind, O. Nathan, & A. S. Pentland (2015), "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE SecurityPrivacy Workshop, San Jose, CA, USA, 2015, pp. 180–184.

[18] X. Liang et al (2017)., "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in Proc. 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. (CCGRID), Madrid, Spain, 2017, pp. 468–477.

[19] www.scopus.com (Data access till Feb. 22nd, 2021).