Spring 1-30-2021

Bibliometric survey on Zero-Knowledge Proof for Authentication

Adwait Pathak
Pimpri Chinchwad College of Engineering, Pune, India, pathakap21@gmail.com

Tejas Patil
Pimpri Chinchwad College of Engineering, Pune, India, tejas.svpatil@gmail.com

Shubham Pawar
Pimpri Chinchwad College of Engineering, Pune, India, imshubhampawar4@gmail.com

Piyush Raut
Pimpri Chinchwad College of Engineering, Pune, India, piyushraut1608@gmail.com

Smita Khairnar
Pimpri Chinchwad College of Engineering, Pune, India, chavansmita31@gmail.com

See next page for additional authors

Authors
Adwait Pathak, Tejas Patil, Shubham Pawar, Piyush Raut, Smita Khairnar, and Dr. Shilpa Gite

Bibliometric survey on Zero-Knowledge Proof for Authentication

Adwait Pathak[1], Tejas Patil[2], Shubham Pawar[3], Piyush Raut[4],Smita Khairnar[5], Dr. Shilpa Gite[6]

[1,2,3,4] Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India.

Email:

[1]pathakap21@gmail.com, [2]tejas.svpatil@gmail.com, [3]imshubhampawar4@gmail.com, [4]piyushraut1608@gmail.com

[5]Professor, Dept. of Computer Engineering, Pimpri Chinchwad College of Engineering, Pune, India.

Email: [5]chavansmita31@gmail.com

[6]Assistant Professor, CS Department, Symbiosis Institute of Technology(SIT), Lavale, Pune, Faculty, Symbiosis Centre for Applied Artificial Intelligence(SCAAI), Symbiosis International (Deemed University), Pune, India.

Email: [6]shilpa.gite@sitpune.edu.in

ABSTRACT

Background: Zero Knowledge Proof is a persuasive cryptographic protocol employed to provide data security by keeping the user's identity, using the services anonymously. Zero Knowledge Proof can be the preferred option to use in multiple circumstances. Instead of using the public key cryptographic protocols, the zero-knowledge proof usage does not expose or leak confidential data or information during the transmission. Zero Knowledge Proof protocols are comparatively lightweight; this results in making it efficient in terms of memory. Zero Knowledge Proof applications can reside in authentication, identity management, cryptocurrency transactions, and many more. Traditional authentication schemes are vulnerable to attacks like password attacks, man-in-the-middle, replay attack, etc. while data transmission takes place over the network. Hence, there is a high need for developing an authentication scheme that does not leak the confidential information and provides authentication without disclosing the identity.

Conclusion: In this paper the bibliometric study of Zero Knowledge Proof for Authentication is performed by using data extracted from the Scopus database. Observations are made based on this study that the maximum research publications on Zero Knowledge Proof for Authentication are from China, United States and India respectively. The conclusion of the paper is drawn that this specific research field is latest and research work in the coming years is necessary on Zero Knowledge Proof for Authentication.

Keywords: Authentication, Zero knowledge Proof, ZKP, Cybersecurity, security, survey, Bibliometric survey, Bibliometric analysis

1. INTRODUCTION

In today's world, the number of authentication systems has increased because of the increasing number of internet services. The usual method we see or use daily is the username or email and password method. Another variation is the addition of a layer in the form of a one-time password. The user will get an OTP on the phone or any other connected device. This is called two-factor authentication (2FA), where login is authenticated if the username/password and the OTP (one-time password) is valid. The addition of more layers to this system will subsequently be called multi-factor authentication (MFA). Additionally, authentication and authorization using biometrics is growing daily. The usage of fingerprint scanners, face scanners are being commercialized.

The most common authentication model used by the services on the internet is the traditional authentication scheme. Here, the server stores the credentials of the users. These credentials are sent to the server in the plaintext format, so that it can tally the credentials to the one stored in the database. If both are matched, the user is authenticated. The drawbacks of this traditional scheme are that it is privy to many attacks.

The concept of Zero Knowledge Proof is to verify information from one party by the other party without giving out the actual context of the information. This method is used to provide confirmation without letting the verifier know the actual information. A way of authenticating data where there is no exchange of secret keys (passwords), so that they are not stolen, is the zero-knowledge proof method.

(Lum & Jun, 2010) Zero Knowledge Proof systems have three important properties: Soundness, Completeness, Zero-Knowledge. Pertaining to the given example we can explain these traits.

- **Completeness**
- **Soundness**
- **Zero-knowledge**

A bibliometric approach is presented by this paper, to analyse the number of efforts taken earlier by researchers to study the Zero Knowledge Proof for Authentication. The goal of this study is to evaluate the research done globally on using Zero Knowledge Proof for Authentication till date, which will be helpful for future researchers in this specific domain.

Below are the remarkable purposes for the Bibliometric Analysis:

- To illustrate several types of documents in academic publications in the research field.
- The research papers published in numerous languages.
- To study the pattern in which the research papers are published over the defined span of years.
- Analysis based on Geographical locations comprises the distinct countries of the world where the research has been done earlier.
- Top researchers who gave the noteworthy input to the field of research.
- The pattern of the publications depending on the organizations or affiliations.
- The papers that are cited the highest.

This paper contributes a Bibliometric Survey on " Zero Knowledge Proof for Authentication " to increase the security and privacy of traditional authentication methods. In Section 2, the work related to Zero Knowledge Proof for Authentication using different types of algorithms is presented. The collection of data related to Zero Knowledge Proof for Authentication is featured in Section 3. Section 4, illustrates the data extracted from the Scopus database. Network analysis, and Statistical analysis, are the two types of analysis that were performed in this section. Section 5, describes the limitations and the Conclusion of the survey is drawn in Section 6, followed by the citations of the references at the last.

2. RELATED WORKS

The literature survey on Zero-Knowledge Proof for Authentication is further classified into two types. This will be distributed as "Zero-Knowledge Proof for Authentication using Diffie-Hellman Key Exchange Algorithm and Zero-Knowledge Proof for Authentication using Public Key Encryption".

2.1 Zero-Knowledge Proof Authentication Protocol

(Soewito and Marcellinus 2020) talks about how the Internet of Things devices can be equipped with combined key exchange using authentication based on identity and zero knowledge. Various ways have been suggested to overcome the challenges of IoT devices. (H. Liu and Ning 2011) also talks about how ZKP can be included in IoT devices and also providing security for the data being transmitted. (Ma, Ge, and Zhu 2014) proposes a scheme where RFID can be implemented using light weight ZKP. The issue addressed is important because RFID applications are becoming ubiquitous. ZKP also finds applications in Wireless body area networks (WBAN). WBAN has high capability in the healthcare industry. [3] talks about how WBAN and ZKP can be combined. It proposes the design of an energy efficient authentication method, which is secure and lightweight, called BANZKP for the same purpose. (W. Liu, Wang, and Peng 2020) has proposed a secure and remote MFA scheme that has three aspects: identity of the user, password and biometrics of the user. The remote server authenticates these. According to their experiment and simulation of the result, this proposed scheme is very efficient in the upcoming 5G communication environment as well as the potent smart devices. (Grzonkowski 2010) has dealt with using ZKP for mobile and cloud services authentication. The paper talks about a modified version of ZKP, called "SeDiCi 2.0" which offers mutual as well as two factor authentication.

2.2 Zero-Knowledge Proof Authentication Protocol using Diffie-Hellman Key Exchange Algorithm

The development of Diffie–Hellman (D-H) key exchange algorithm was done for exchanging the secret keys through the insecure channels. In a research work done by (Marím-Fernández, Caballero-Gil, 2016), "a novel scheme based on the idea of non-interactive zero-knowledge proofs is presented". The implemented system only needs to send a message for sharing the information that is confidential in an authenticated manner. The authors have proposed an algorithm to create session keys that are secret and authenticated among the pairs of nodes which are legitimate. Here, Diffie-Hellman protocol is used in the new algorithm for creating the secret key which is shared. Thus, this research work gives an overview of using Zero Knowledge Proof for Authentication with Diffie-Hellman key exchange algorithm.

(Ibrahem 2012) has modified the Diffie-Hellman key exchange algorithm to an "interactive zero-knowledge proof protocol". The authors have implemented a protocol for satisfying the properties of zero knowledge proof and for countering the familiar vulnerable attacks. The proposed system here helps in countering the man-in-the-middle attack. Further, a survey done by (Pathak et al. 2020) explains the "framework of IoT security" and the "known vulnerabilities" of it. The authors also present the threats that exist in various layers of IoT application. Different solutions are also stated by the authors which include the use of

“lightweight encryption.” This survey gives a brief overview of “security framework in IoT and attacks on IoT environment.”

(Flood and Schukat 2014) have designed a system to improve privacy and data integrity and also to provide the authentication between the peers in an IoT environment. Their proposed system uses zero knowledge proof with Diffie-Hellman key exchange algorithm. The advantages of doing so are, mutual authentication is provided and a public key transport mechanism is combined for complementary key negotiation protocol. When the Diffie-Hellman key exchange algorithm is implemented strongly, it “requires public keys in the order of 768 or 1024 bits” this gives relevant key exchange rounds in mix with protocol.

2.3 Zero-Knowledge Proof Authentication Protocol using Password-Authenticated Key Exchange

A PAKE protocol, initially described by Bellovin and Merritt, is a unique form of cryptographic key exchange protocol and has received considerable cryptographic attention since then. The (Yassin et al., 2012) proposal holds several advantages: password privacy preservation and session key secrecy. There is no requirement for registering the passwords of the users. There is no need for the user to register its credentials. By taking into account three prominent factors: data owner, users, and service provider. The owner of that data is responsible for performing confident decisions in order that the essential keys are given to different components.

(Yi et al., 2019) A new method is known as TPASS is introduced in this paper. TPASS is Threshold password-authenticated secret sharing. This is employed for securing the data of the user on the cloud. Before the data is uploaded on a data server in the cloud,the user itself encrypts it with a random key. This random key is then shared secretly along with the password with n key servers in the cloud. Now, whenever a user downloads data, it is encrypted by the server. In order to decrypt this data, the user can recover the random key from the servers in the cloud. For this process, the user will only require his password. The use of this key exchange allows the users to acknowledge over new session keys with every data server.

(Hao, 2014) discusses the various Public-Key Authenticated Key Exchange protocols. The PK-AKE family based on digital signatures is looked into. Presented are the variations of the Diffie-Hellman and various other protocols’ flaws and positives. (Lancrenon et al.,2016) have proposed two different versions of J-PAKE known as RO-J-PAKE and CRS-J-PAKE. The advantage of these versions is that they make use of two less zero knowledge proofs as compared to the original protocol. The authors have analyzed the capability of three protocols and showed these two variants as being more efficient than J-PAKE.

(Chuat et al., 2020) This paper was the incentive for us to pursue the topic of authentication using ZKP. This paper provides the boundaries of the traditional authentication system and why Zero-knowledge proof systems should supplant them. The approach of implementing authentication in this paper is by the application of SRP, AugPAKE. Initialization, Authentication, Authorization, Session Management is explained using the following scheme.

3. PRELIMINARY DATA COLLECTION

There exists various prominent means for accessing the research papers and review articles. In order to access the research data, many publication resources such as ResearchGate, Mendeley, Scopus, DBLP, Google Scholar, SCI Imago, Clarivate, ScienceDirect are available. The Scopus is a vast, eminent and most prestiged dataset. Hence, the database which has been selected for the Bibliometric analysis is the Scopus. (Bagane and Kotrappa 2020)

3.1 Search Procedure

The research articles in the Scopus database are searched using the different keywords. These keywords, which are used are divided further in two types: Master keywords and Secondary keywords. The Master keywords and Secondary keywords used on Zero Knowledge Proof for Authentication, are stated in Table 1. The Master keyword “zero knowledge proof " which is the common keyword, gives 1,104 (Access on 21st Jan 2021) of the Scopus documents.

Table 1. The search keywords selected for Zero Knowledge Proof for Authentication.

Primary keyword	**“zero knowledge proof”**
Secondary keyword using (AND)	**“authentication”**

For this specific study, the research is limited to the span of years from 2010 to 2021. To search the research articles in the Scopus database, the precise query is:

```
TITLE-ABS-KEY ( "zero knowledge
proof" AND "authentication" ) AND PUBYEAR > 2009 AND PUBYEAR < 2022
```

3.2 Preliminary Search Results

The query stated in Section 3.1, found 329 research documents on the Scopus database. Table 2. shows different document types of research publications on Zero Knowledge Proof for Authentication research. 57.44% of the researchers have published their research articles in conference paper, subsequently by articles, with 35.86% of the total research documents. Conference review has 4.55% of the total research documents published. Book, book chapter and review, have very few additions in the total number of documents with 0.91%, 0.6% and 0.6% respectively.

Table 2. Different document types published on Zero Knowledge Proof for Authentication.

Document Type of the publications	**Number of the publications**	**Contribution Percentage**
Conference Paper	189	57.44%
Article	118	35.86%
Conference Review	15	4.55%
Book	3	0.9%
Book Chapter	2	0.6%
Review	2	0.6%
Total	329	100%

Dataset access information source: http://www.scopus.com (accessed January 21, 2021)

Analysis is also done on the language type that is used for publishing the research documents. Table 3, states the contribution depending on the language used for the documents for Zero Knowledge Proof for Authentication. In Table 3, observations are, English is the prominent language used by the researchers for publishing their work. Followed by Chinese. Very less papers are published in the French, Russian and Turkish languages.

Table 3. Different languages used for publications in Zero Knowledge Proof for Authentication.

Language used in publication documents	**Publication Count**
English	307
Chinese	19

French	2
Russian	1
Turkish	1

Dataset access information source: http://www.scopus.com (accessed on January 21, 2021)

3.3 Exploratory Data Highlights

The documents are selected on Zero Knowledge Proof in designing Authentication systems, and keywords are in the range of years from 2010 to 2021. Table 4, shows the pattern of the publication count year wise Zero Knowledge Proof for Authentication. The interpretation of this data indicates that most of the research has taken place in the year 2020. In Table 4, a clear observation can be made that the input to the research was comparatively very minimal during the years 2010 to 2013.

Table 4. Publication patterns year wise on wise Zero Knowledge Proof for Authentication.

Year	**Publication Count**
2021	2
2020	60
2019	44
2018	31
2017	31
2016	29
2015	27
2014	30

2013	18
2012	24
2011	18
2010	15

Data access information source: http://www.scopus.com (accessed on January 21, 2021)

Figure 1, depicts the result in the form of Radar chart for the year wise publication count pattern Table 4. The chart represents the dominant year 2020, which has the highest publication count of the total of 60 published research documents in Zero Knowledge Proof for Authentication.

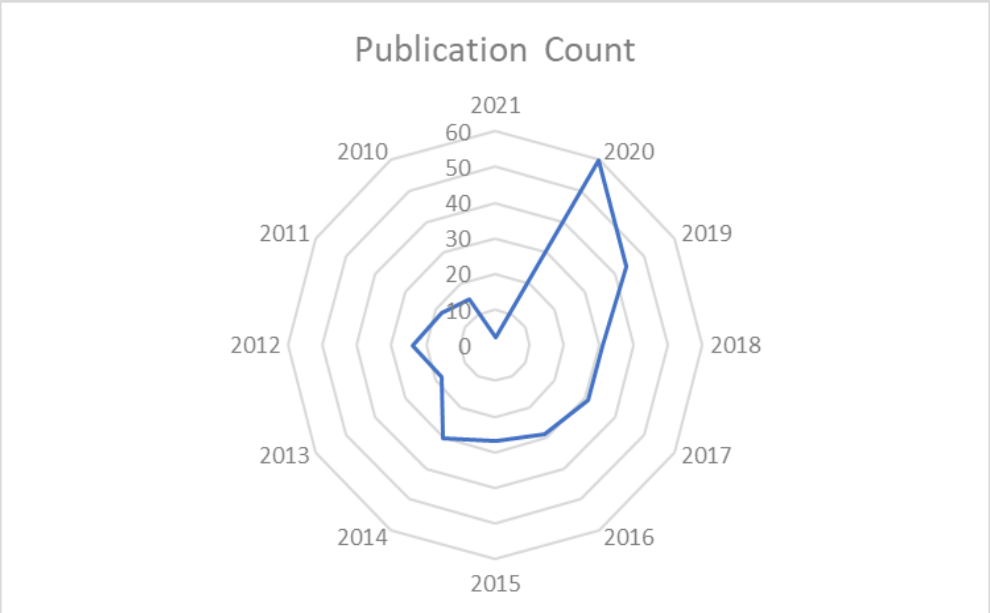

Figure 1. Publication count patterns year wise on wise Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4. BIBLIOMETRIC SURVEY

This section consists of the detailed Bibliometric analysis for understanding the literature with its diversity and more about the researchers and their work done with the help of appropriate keywords for wise Zero Knowledge Proof for Authentication. Representations are done by the help of visuals like various charts and graphs for showing the wide spread of the research based on geographical locations and countries. It is also done on the affiliations to the organizations and the institutions.

There are two different approaches for carrying out the Bibliometric Survey for Zero Knowledge Proof for Authentication.

- Network analysis mainly depends on geographical locations, publication title, source of the title, keywords, year of the publication, and collaboration in the authors, count of citation, etc.
- Statistical analysis mainly depends on the inputs of countries to the research field, input by the subject, authors, author's collaborations, source type and source titles.

4.1 Analysis Based on Geographic Locations

The analysis is also done based on the geographic location with the help of Microsoft Excel Map. Here, input is given as two columns, country name and the count of the publications by that country. Once this data is selected, a geographical map is created based on the data, which represents the count of papers on the specific geographical-location. According to the geographical world map, China has published the maximum number of papers, which is 85.

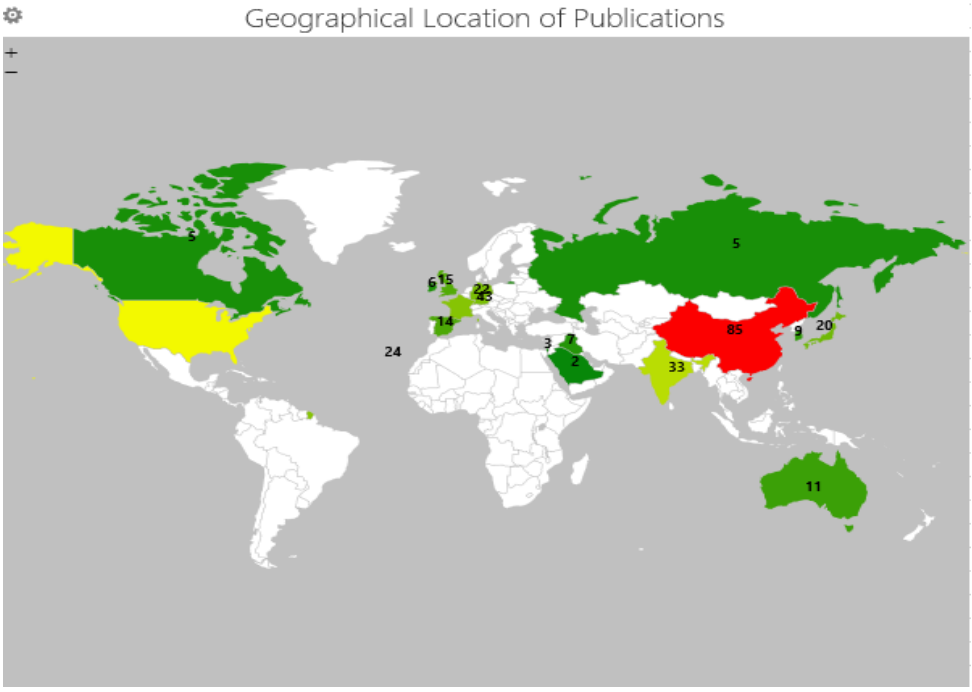

Figure 2. Geographical location of publications. **Data access information source: http://www.scopus.com (accessed on January 21, 2021)**

Figure 3 depicts using pie-chart, the countries in the research on Zero Knowledge Proof for Authentication. The observations are that China contributes 25.83%. The second

contributors are the United States and India with 13.06% and 10.03% of contribution respectively. It is also observed from the chart that Saudi Arabia has the lowest contribution of all.

Figure 3. Countries publishing research on Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4.2 Statistical Analysis Based on Keywords

In Table 5, the top ten keywords for searching the Scopus database for Zero Knowledge Proof for Authentication, are shown. With the application of appropriate combinations of the selected keywords, the papers for the particular research field can be selected and filtered. It is seen from Table 5 that, "Authentication" keyword is used most extensively.

Table 5. Top ten keywords for Zero Knowledge Proof for Authentication.

Keyword	**Publication Count**
Authentication	266
Zero Knowledge Proof	194
Cryptography	131
Network Security	105

Data Privacy	43
Public Key Cryptography	40
Zero-knowledge Proof	40
Non-interactive Zero-knowledge Proofs	38
Blockchain	31
Electronic Document Identification Systems	30

Data access information source: http://www.scopus.com (accessed on January 21, 2021)

Figure 4. displays a visual illustration in form of a Word Cloud created with the keywords for Zero Knowledge Proof for Authentication.

Figure 4. Word Cloud illustration of keywords used for Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4.3 Network Analysis

Network analysis displays the association between the various parameters that put up values for the computation. Network analysis is represented by the graphical illustrations. In this paper, the several network analysis illustrations are created using VOSviewer. The network analysis illustrations with different attributes for Zero Knowledge Proof for Authentication, are displayed by Figure 5 and 6.

VOSviewer is a free tool. It can be downloaded from the VOSviewer website. VOSviewer is used to analyze the various parameters using a Bibliometric network. The input to the VOSviewer needs to be (.csv) file. There are three types of visualization analysis with VOSviewer, they are Network visualization, Overlay Visualization, and Density visualization.

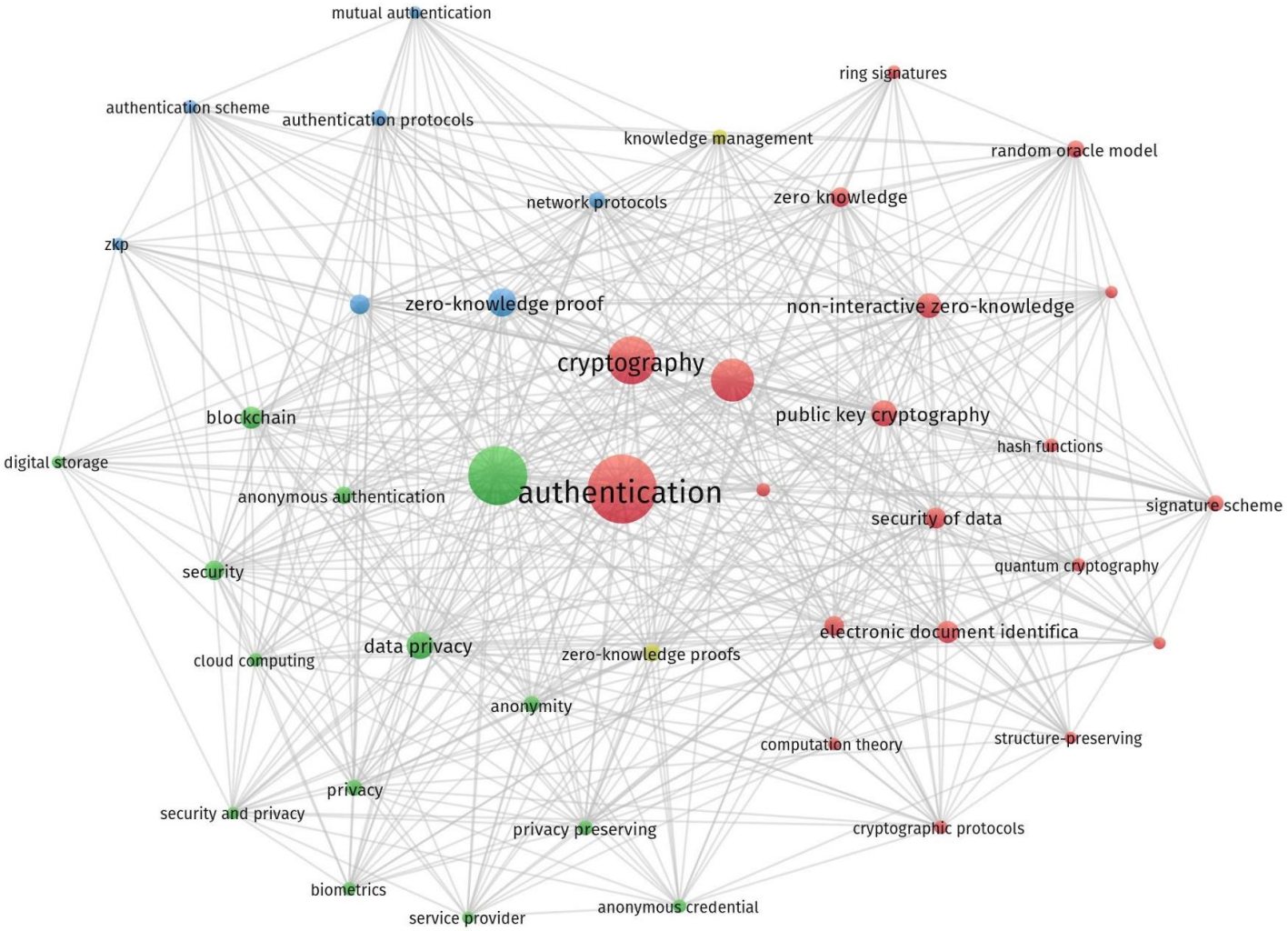

Figure 5: Network visualization illustration by using keywords and source title, keywords from Scopus dataset.

Data access information source: http://www.scopus.com (accessed on January 21, 2021) (Image Source: https://www.vosviewer.com)

Visualization between the keywords and the source titles is shown in Figure-5, from the extracted Scopus data. The keywords which are extracted from the source title are depicted by the circles in the figure. The occurrence of the keyword is shown by the size of the circle. The association between the keywords is represented by the links amid circles. Here, lesser distance depicts stronger association and wider distance depicts weaker association. The same colours are used to represent the keywords which are closely related to each other and different colours are used to represent different groups. The keyword and the size of the circle is depicted by the label. The weight of the keyword decides the label. The bigger the size of the label, the higher is the weight of the keyword and vice versa. The words are linked with each other by the lines present amid them.

Figure 6, displays the visualization and also the citations of the documents. The analysis is done by selecting a minimum of two citations for each document. The 329 number of documents were selected and the citation link calculation was carried out.

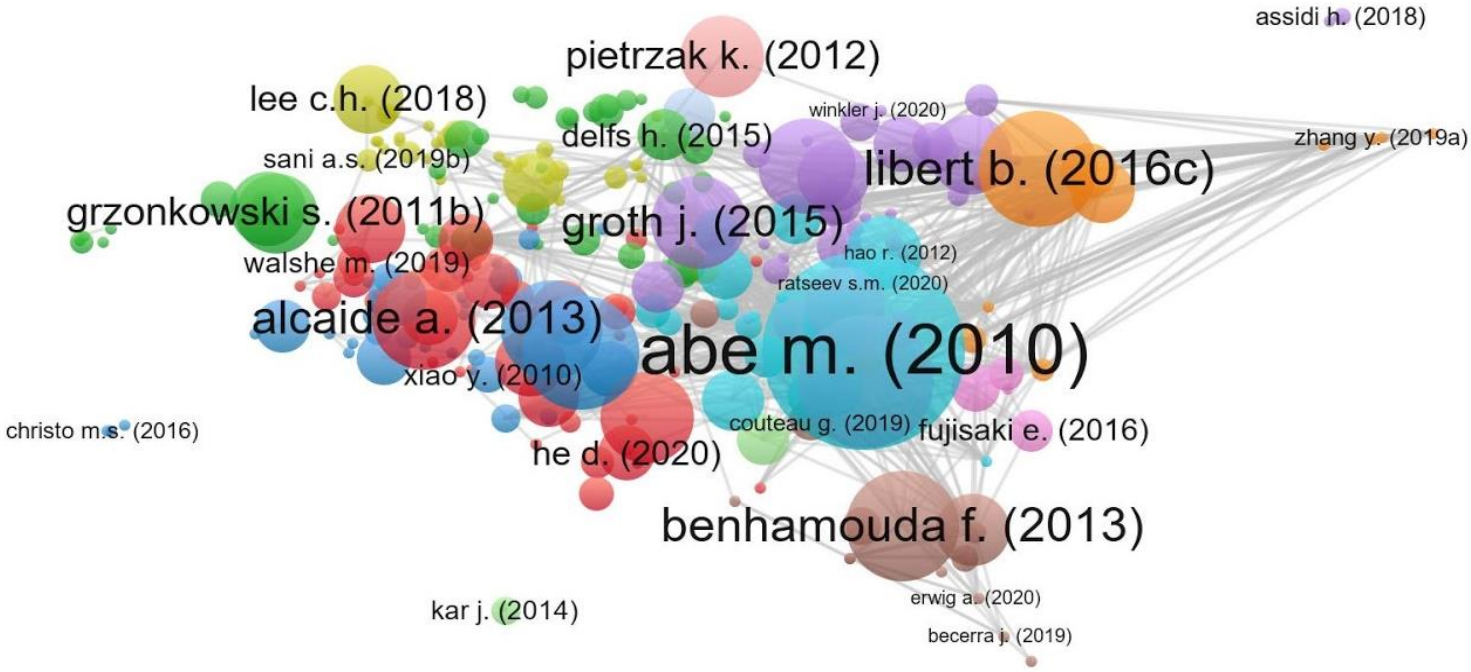

Figure 6: Network visualization of the document and the citations received by document using Scopus dataset.

Data access information source: http://www.scopus.com (accessed on January 21, 2021) (Image Source: https://www.vosviewer.com)

4.4 Statistical Analysis based on Affiliations

The analysis of the contributions based on the affiliations of the university and organizations is displayed by Figure 7. It displays the top ten organizations who have contributed to the research area of Zero Knowledge Proof for Authentication. The 'CNRS Centre National de la Recherche Scientifique' from France has the maximum contribution in the research field of Zero-Knowledge Proof for Authentication, followed by the 'Xidian University' from China.

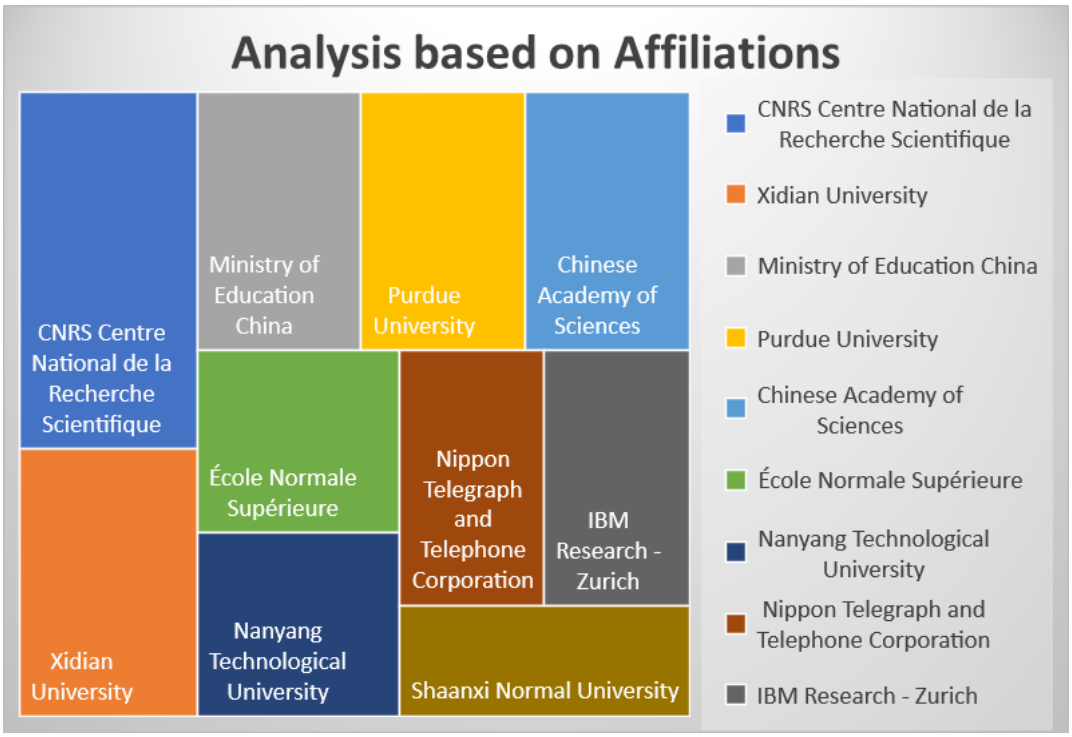

Figure 7. Analysis based on Affiliations on Zero Knowledge Proof for Authentication.
Source: http://www.scopus.com (accessed January 21, 2021)

4.5 Statistical Analysis based on Subject Areas

The dispersion of the publications in different areas for Zero-Knowledge Proof for Authentication is shown by Figure 8. It is observed that almost all research is done in the subject area of 'Computer Science', second by 'Mathematics' and third by 'Engineering'. Also, an observation is made that the least count of publications are published in the 'Energy' subject area.

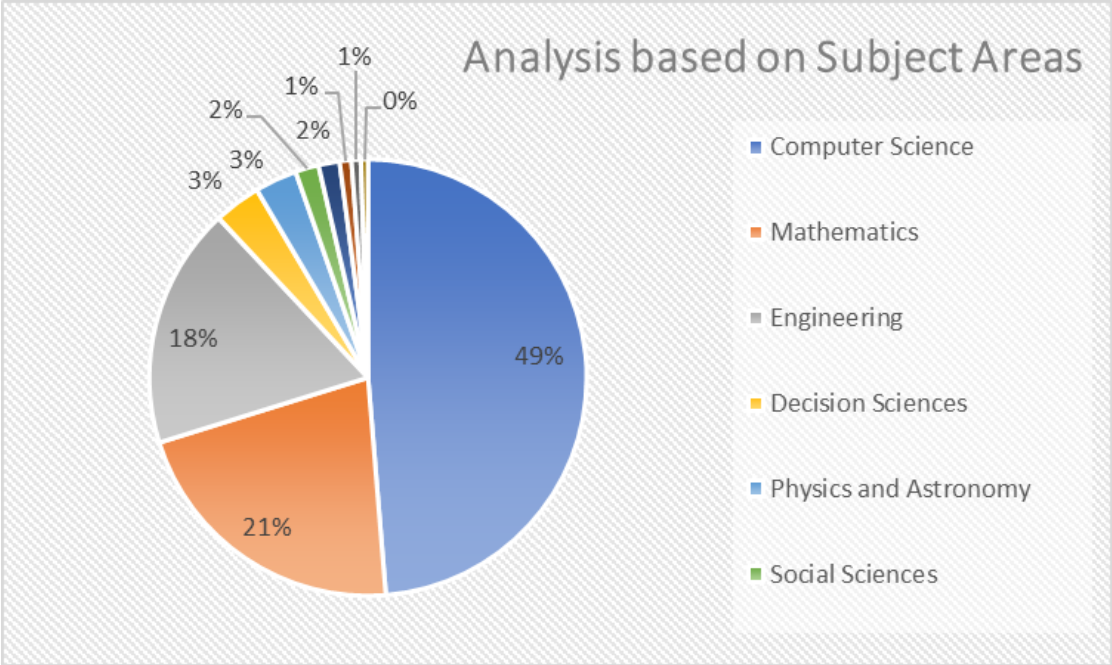

Figure 8. Analysis based on subject areas on the extracted data on Zero Knowledge Proof for Authentication. **Data access information source: http://www.scopus.com (accessed on January 21, 2021)**

4.6 Statistical Analysis based on Authors

The contribution in the research area of Zero Knowledge Proof for Authentication by the top ten authors is shown in Figure 9. The author Elisa Bertino from Purdue University, United States, has published eight papers, followed by author Yupeng Zhang from University of Maryland, United States, who has published six papers. The third top most author is Hasini Gunasinghe from Sabaragamuwa University of Sri Lanka. She has published five papers.

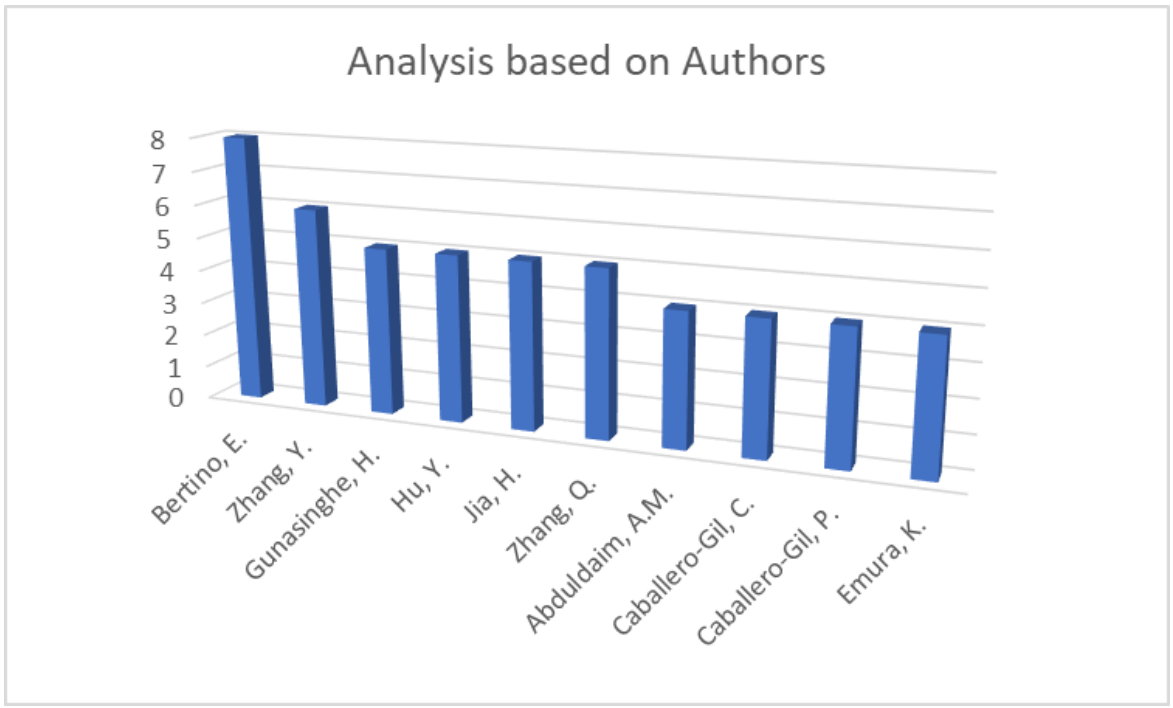

Figure 9. The contribution of top ten authors in the research field of Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4.7 Statistical Analysis based on Document Types

Figure 10, represents the type of documents that are published in the research areas of Zero Knowledge Proof usage in Authentication. From the data extracted from the Scopus database of Zero Knowledge Proof in designing Authentication systems, observation is clear . 57.44% of the researchers have published their research articles in conference paper, subsequently by articles, with 35.86% of the total research documents. Conference review has 4.55% of the total research documents published. Book, book chapter and review, have very few additions in the total number of documents.

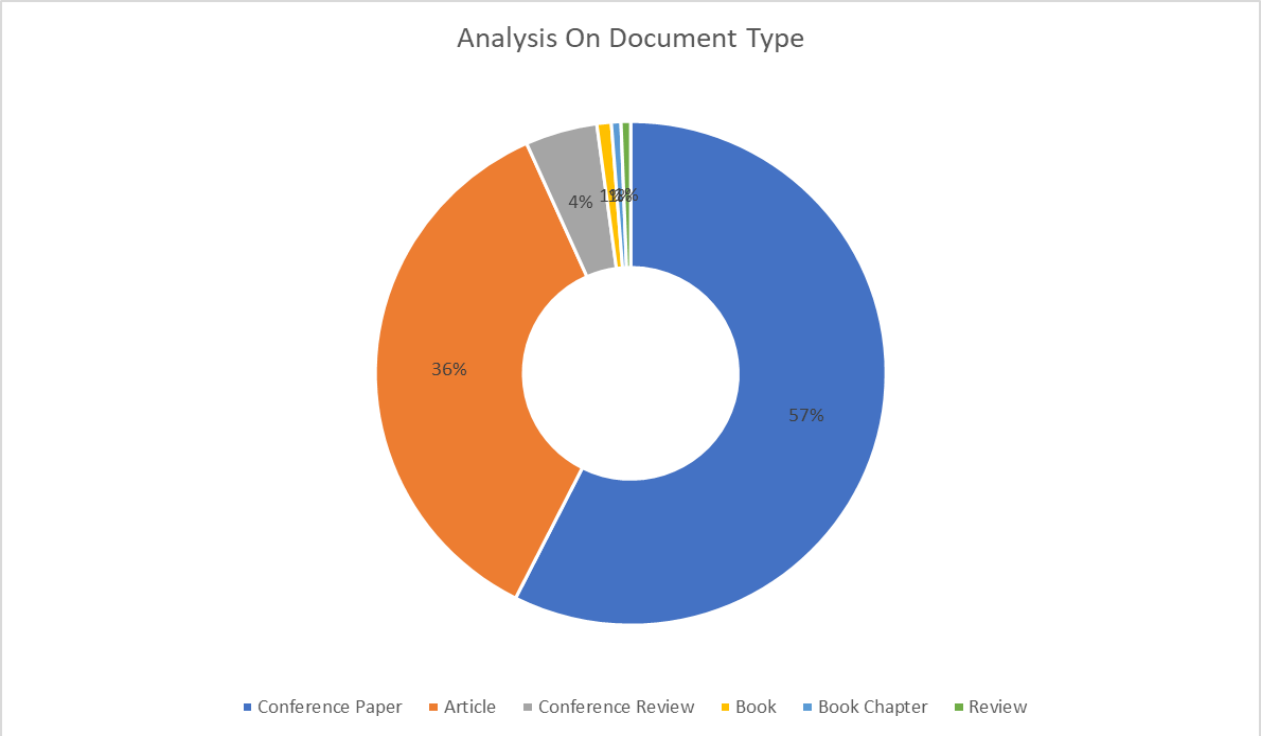

Figure 10. Different document types published on Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4.8 Statistical Analysis based on Source Titles

Figure 11, shows the analysis based on the sources of the documents. It can be observed from Figure 11, that Lecture Notes in Computer Science, including Subseries Lecture Notes in Artificial Intelligence and also Lecture Notes in Bioinformatics has most research work published. Globecom IEEE Global Telecommunications Conference has the least number of publications in the research field of Zero Knowledge Proof for Authentication.

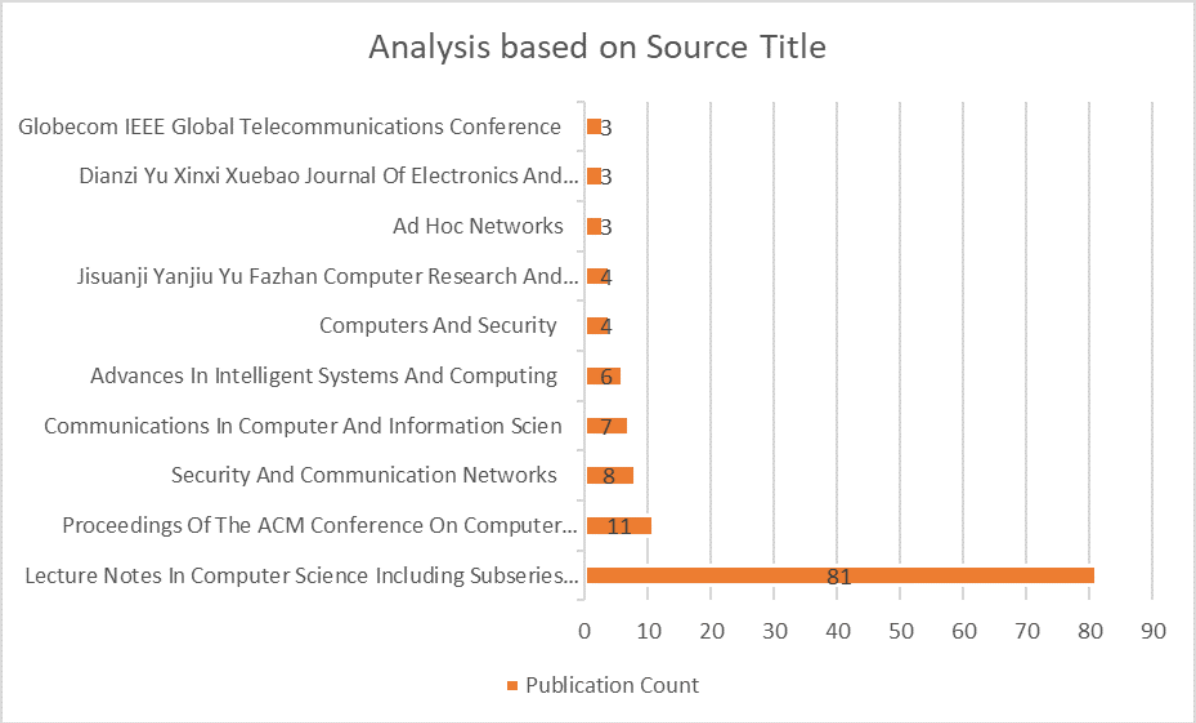

Figure 11. Analysis based on sources of the documents published on Zero Knowledge Proof for Authentication. Data access information source: http://www.scopus.com (accessed on January 21, 2021)

4.9 Analysis based on Funding Sponsors

The analysis based on the funding sponsors of the publications is represented by Figure 12. The National Natural Science Foundation of China has given most sponsorship funding for the research area of Zero Knowledge Proof for Authentication. The least funded sponsor is Deutsche Forschungsgemeinschaft.

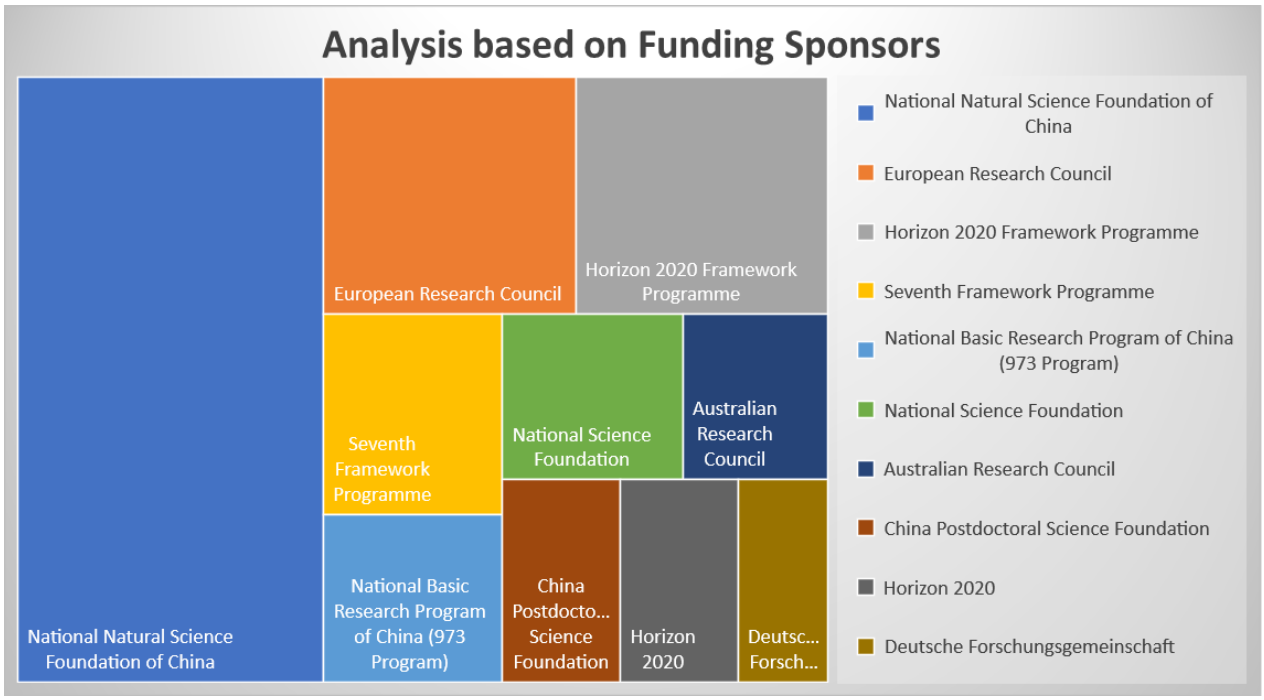

Figure 12. Analysis based on funding sponsors of the documents on Zero Knowledge Proof for Authentication.

Source: http://www.scopus.com (accessed on January 21, 2021)

4.10 Analysis based on publication citations

Table 7 shows the citations done for the top twenty publications for this particular research. The representation is done year wise for the publications on Zero Knowledge Proof for Authentication. The total count of the citations is 1207 for 329 published documents. It is clearly observed from Table 6 that the research publications in this area got the highest number of citations in the year 2019, which is 243 citations. The count of the citations is less up to year 2014. The maximum citations are seen in 2019 and 2020.

It is deduced that the research publication with the title **"Structure-preserving signatures and commitments to group elements"** has the maximum citations in this field of Zero Knowledge Proof for Authentication.

Table 6: Analysis based on the citations year wise.

Year	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
No. of citations	3	20	33	45	72	110	133	154	182	243	204	8

Data access information source: http://www.scopus.com (accessed on January 21, 2021)

Table 7. Citation analysis overview for top twenty publications on Zero Knowledge Proof for Authentication.

Sr. No	Document Title	<2016	2016	2017	2018	2019	2020	2021	Sub total	Total
		283	133	154	182	243	204	8	924	1207
1	*Structure-preserving signatures and commitments to group elements*	130	22	26	34	21	11	0	94	224
2	*Tightly secure signatures and public-key encryption*	27	17	13	14	19	14	1	78	105
3	*Zero-knowledge arguments for lattice-based accumulations: Logarithmic-size ring signatures and group signatures without trapdoors*	0	3	9	21	31	17	0	81	81
4	*A privacy-preserving attribute-based authentication system for mobile health networks*	11	13	15	18	13	7	0	66	77
5	*New techniques for SPHFs and efficient one-round PAKE protocols*	18	18	12	6	10	7	1	54	72
6	*Anonymous authentication for privacy-preserving IoT target-driven applications*	6	9	10	7	16	13	1	56	62
7	*PAAS: A privacy-preserving attribute-based authentication system for eHealth networks*	20	7	12	12	5	3	0	39	59
8	*Post-quantum zero-knowledge and signatures from symmetric-key primitives*	0	0	1	15	19	19	0	54	54
9	*One-out-of-many proofs: Or how to leak a secret and spend a coin*	1	6	3	12	12	19	0	52	53
10	*Password-protected secret sharing*	16	9	6	6	7	7	0	35	51
11	*A Secure and Efficient Communication Scheme with Authenticated Key Establishment Protocol for Road Networks*	0	1	16	10	10	11	0	48	48
12	*Cryptography from learning parity with noise*	7	5	9	6	7	7	0	34	41

13	*Sharing cloud services: User authentication for social enhancement of home networking*	13	9	5	5	5	3	0	27	40
14	*A post-quantum digital signature scheme based on super singular isogenies*	0	0	0	11	17	11	0	39	39
15	*Fast secure two-party ECDSA signing*	0	0	0	7	12	17	1	37	37
16	*Security analysis of authentication protocols for next-generation mobile and CE cloud services*	10	8	5	6	3	3	0	25	35
17	*Identity-based aggregate and multi-signature schemes based on RSA*	21	4	3	6	1	0	0	14	35
18	*Disjunctions for hash proof systems: New constructions and applications*	3	2	9	5	6	8	0	30	33
19	*Improved non-interactive zero knowledge with applications to post-quantum signatures*	0	0	0	0	12	19	0	31	31
20	*Implementation of IoT system using block chain with authentication and data protection*	0	0	0	1	17	8	4	30	30

Source: http://www.scopus.com (accessed on January 21, 2021)

5. LIMITATIONS OF THIS STUDY

In this bibliometric study, just Scopus database is taken into consideration for selecting the publications having the combination of keywords. Different databases exist like Web of Science, Google Scholar and PubMed, for searching the research publications. These different databases could have been used too for the collection of research publications. Using different databases gives various statistical analysis based on the publication citations. In this bibliometric study, only Scopus database citations are considered for analysis. Here in this study, the only language used is English. Only particular keywords are used by the research scholars. Different combinations of the keywords, by adding or removing the words that have the same meaning can be tried on the database. This bibliometric study considers a specific span of years that is from 2010 to 2021, obviously this study doesn't count the research work done before the defined span of years. Therefore, this research study has a scope for future work to be done.

6. CONCLUSION

Through the analysis done in this bibliometric study, it is noted that different research work is done in the concept of using Zero Knowledge Proofs to create novel Authentication systems. It is observed from the analysis done that Zero Knowledge Proof, to design Authentication systems, is a serious research topic in the field of research, specifically in the countries of China, India and United States. This bibliometric survey is done on the data extracted from 329 research publication documents from Scopus database, in the defined period of years 2010-2021. In order to search the research documents, "zero knowledge proof" and "authentication" keywords are used. This study tells that the earlier research is mainly done in the subject area of "Computer Science" having the maximum count of publications in Lecture Notes In Computer Science, including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics journal. The National Natural Science Foundation of China has granted the highest funding in this specific research field. China advances in this research area with its publications with the United States and India following it. A growth is observed in the count of publications from the year 2019, this suggests an expansion in this research field in the coming years. Nevertheless, extensive scope of innovations can be carried out in this research field. There is a necessity for the constant advancement in research.

7. REFERENCES

[1] M. Abdalla, F. Benhamouda, and P. MacKenzie, “Security of the J-PAKE password-authenticated key exchange protocol,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2015-July, pp. 571–587, 2015, doi: 10.1109/SP.2015.41.

[2] P. A. Bagane and D. Kotrappa, “Bibliometric Survey for Cryptanalysis of Block Ciphers towards Cyber Security,” *Libr. Philos. Pract.*, p. 1, 2020.

[3] P. Flood and M. Schukat, “Peer to peer authentication for small embedded systems: A zero-knowledge-based approach to security for the Internet of Things,” *DT 2014 - 10th Int. Conf. Digit. Technol. 2014*, pp. 68–72, 2014, doi: 10.1109/DT.2014.6868693.

[4] S. Grzonkowski, *SeDiCi: An authentication service taking advantage of zero-knowledge proofs*, vol. 6052 LNCS. 2010.

[5] S. Grzonkowski, P. M. Corcoran, and T. Coughlin, “Security analysis of authentication protocols for next-generation mobile and CE cloud services,” *Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron.*, pp. 83–87, 2011, doi: 10.1109/ICCE-Berlin.2011.6031855.

[6] H. Gunasinghe and E. Bertino, “PrivBioMTAuth: Privacy Preserving Biometrics-Based and User Centric Protocol for User Authentication from Mobile Phones,” *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 1042–1057, 2018, doi: 10.1109/TIFS.2017.2777787.

[7] F. Hao, “On robust key agreement based on public key authentication,” *Secur. Commun. Networks*, vol. 7, no. 1, pp. 77–87, 2014, doi: 10.1002/sec.550.

[8] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, “Secure and Efficient Two-Party Signing Protocol for the Identity-Based Signature Scheme in the IEEE P1363 Standard for Public Key Cryptography,” *IEEE Trans. Dependable Secur. Comput.*, vol. 17, no. 5, pp. 1124–1132, 2020, doi: 10.1109/TDSC.2018.2857775.

[9] D. Hofheinz and T. Jager, “and Public-Key Encryption,” pp. 590–607, 2012.

[10] M. K. Ibrahem, “Modification of Diffie-Hellman key exchange algorithm for Zero knowledge proof,” *2012 Int. Conf. Futur. Commun. Networks, ICFCN 2012*, pp. 147–152, 2012, doi: 10.1109/ICFCN.2012.6206859.

[11] N. Khernane, M. Potop-Butucaru, and C. Chaudet, “BANZKP: A Secure Authentication Scheme Using Zero Knowledge Proof for WBANs,” *Proc. - 2016 IEEE 13th Int. Conf. Mob. Ad Hoc Sens. Syst. MASS 2016*, pp. 307–315, 2017, doi: 10.1109/MASS.2016.046.

[12] J. Lancrenon, M. Škrobot, and Q. Tang, “Two more efficient variants of the J-PAKE protocol,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9696, pp. 58–76, 2016, doi: 10.1007/978-3-319-39555-5_4.

[13] X. J. Lin, L. Sun, and H. Qu, “Insecurity of an anonymous authentication for privacy-preserving IoT target-driven applications,” *Comput. Secur.*, vol. 48, pp. 142–149, 2015, doi: 10.1016/j.cose.2014.08.002.

[14] H. Liu and H. Ning, “Zero-knowledge authentication protocol based on alternative mode in RFID systems,” *IEEE Sens. J.*, vol. 11, no. 12, pp. 3235–3245, 2011, doi: 10.1109/JSEN.2011.2160052.

[15] W. Liu, X. Wang, and W. Peng, “Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things,” *IEEE Access*, vol. 8, pp. 8754–8767, 2020, doi: 10.1109/ACCESS.2019.2962912.

[16] X. Liu, M. Guo, B. Zhang, and X. Li, "An efficient attribute-based authentication scheme with multiple authorities in public cloud," *J. Phys. Conf. Ser.*, vol. 1607, no. 1, 2020, doi: 10.1088/1742-6596/1607/1/012043.
[17] L. Ma, Y. Ge, and Y. Zhu, "TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wirel. Pers. Commun.*, vol. 77, no. 2, pp. 1077–1090, 2014, doi: 10.1007/s11277-013-1555-4.
[18] L. Ma, Y. Ge, and Y. Zhu, "TinyZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wirel. Pers. Commun.*, vol. 77, no. 2, pp. 1077–1090, 2014, doi: 10.1007/s11277-013-1555-4.
[19] W. Major, W. J. Buchanan, and J. Ahmad, "An authentication protocol based on chaos and zero knowledge proof," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3065–3087, 2020, doi: 10.1007/s11071-020-05463-3.
[20] F. Marím-Fernández, P. Caballero-Gil, and C. Caballero-Gil, "Authentication based on non-interactive zero-knowledge proofs for the internet of things," *Sensors (Switzerland)*, vol. 16, no. 1, 2016, doi: 10.3390/s16010075.
[21] S. J. Mohammed and S. A. Mehdi, "Web application authentication using ZKP and novel 6D chaotic system," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 20, no. 3, pp. 1522–1529, 2020, doi: 10.11591/ijeecs.v20.i3.pp1522-1529.
[22] A. Pathak, T. Patil, S. Pawar, P. Raut, and S. Khairnar, "A Survey on methodologies for intensifying the security in IOT," vol. 7, no. 19, pp. 1135–1147, 2020.
[23] I. Simsek and E. P. Rathgeb, "Zero-Knowledge and Identity-Based Authentication and Key Exchange for Internet of Things," *IEEE 5th World Forum Internet Things, WF-IoT 2019 - Conf. Proc.*, pp. 283–288, 2019, doi: 10.1109/WF-IoT.2019.8767235.
[24] B. Soewito and Y. Marcellinus, "IoT security system with modified Zero Knowledge Proof algorithm for authentication," *Egypt. Informatics J.*, no. xxxx, pp. 1–8, 2020, doi: 10.1016/j.eij.2020.10.001.
[25] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "A practical privacy-preserving password authentication scheme for cloud computing," *Proc. 2012 IEEE 26th Int. Parallel Distrib. Process. Symp. Work. IPDPSW 2012*, pp. 1210–1217, 2012, doi: 10.1109/IPDPSW.2012.148.
[26] X. Yi *et al.*, "Efficient threshold password-authenticated secret sharing protocols for cloud computing," *J. Parallel Distrib. Comput.*, vol. 128, pp. 57–70, 2019, doi: 10.1016/j.jpdc.2019.01.013.
[27] Chuat L., Plocher S., Perrig A. (2020), "Zero-Knowledge User Authentication: An Old Idea Whose Time Has Come". In: Anderson J., Stajano F., Christianson B., Matyáš V. (eds) Security Protocols XXVII. Security Protocols 2019. Lecture Notes in Computer Science, vol 12287. Springer, Cham. https://doi.org/10.1007/978-3-030-57043-9_19
[28] Scopus database: www.scopus.com (Data accessed till 21st January 2021)
[29] VOSviewer download website: https://www.vosviewer.com/download