

Review of Internet of Things security protocols – A Bibliometric Analysis

Gardner Mwansa*, Ntlima Mabanza**

*Department of Information Technology, Walter Sisulu University, East London, South Africa

**Department of Information Technology, Central university of Technology, Bloemfontein, South Africa

gmwansa@wsu.ac.za, nmabanza@cut.ac.za

Abstract— The upsurge of the fourth industrial revolution brings about an emergence of cloud-based technologies such as the Internet of Things (IoT). By design, these devices and systems are bound to operate in complex environments that require secure assurances at the same time the need for mechanisms to achieve resilience in an event of threats or attacks. Little attention has been paid to finding evidence about security protocols designed to support IoT devices from cyber-attacks. To accomplish this, however, would necessitate a literature review study on current trends, concerns, and ongoing research in the field of Internet of Things security protocols. This is the void that this paper aims to fill through a bibliometric analysis of scientific paper publications.

Hence, this paper presents a review study that assesses the status of the existing research relating to Internet of Things security protocols. A bibliometric analysis was carried out using R Studio on scientific publications in the field of Internet of Things security protocols for the period between 2016 and 2022 retrieved from Web of Science and Scopus databases. The results from the bibliometric analysis showed that there is active research going on in Internet of Things security protocols and is dominated by the American and Asian continents in terms of research paper publications and the collaboration network while Africa is still lacking behind. Based on these review results, this study has established that research in the field of Internet of Things security protocols is still in its infancy in the African continent compared to other continents. In addition, more work is needed in securing Internet of Things systems through continued protocol development including standardised guidelines so as advance more resilience in securing the operations of the devices.

Keywords— Security Protocols, Internet of Things, Cloud-based technologies, Cybersecurity, Bibliometric analysis.

I. INTRODUCTION

Recent discussions and debate from the academia and industry on the probable impact of the “Fourth Industrial Revolution” raises opportunities of investigating the nature of connectedness of digital devices especially the

interconnectedness of the Internet of Things (IoT). IoT consists of interconnected devices or machines that have the capability of transferring data on a communication network without much of physical human intervention [1]. The devices can generate large amounts of data and are monitored and controlled remotely but this carries new risks: the many interfaces and protocols involved provide many points of failures and security vulnerabilities [1]. This calls for greater understanding of IoT interfaces, protocols and devices, including the complex operational technologies and environments that complicate development and business processes.

IoTs have become like everyday objects used in many operational areas such as personal wellness tracking, home, or vehicle automation etc. By design, they interact with the environment in order to generate data sets that are normally hosted in the cloud [1], [2]. Therefore, the security that must be implemented should take into account of the environment in which the sensors are collecting data. The level of trust attributed to the interaction of the devices and the complexity of its distribution can be of some concern because these devices may be exposed to insecure environments [2].

Considering the fact that IoT devices and their associated systems are rapidly increasing worldwide, a closer understanding of the nature of security protocols and measures to deal with attack surface areas is critical [3]. Traditional defence strategies are failing to successfully counter emerging cloud-based threats and attacks [4]. This emerging threat landscape requires an integrated approach to the solution. Network security is an integral part of any connectivity involving networking regardless of the type, size and nature of the network. The rate at which cyber-attacks are exploiting IoT device vulnerabilities has been increasing while the IoT services remain pervasive [5]. In order to secure data and mitigate threats, a number of protocols, technologies, tools and techniques are involved. Hence, a constant review and analysis of effectiveness of IoT associated security protocols is critical for their secure operation.

Although previous research has shown interest in the IoT security protocols such as seeking security solutions, there has been limited comparative studies on analysis of the research trends on IoT security protocols. The main objective of this paper was to carry out a systematic bibliometric analysis to identify emerging trends in finding evidence about security

protocols designed to support IoT devices from cyber-attacks and to accomplish this goal, a systematic literature review of articles about journal performance, collaboration patterns, and research constituents was conducted, along with an investigation of the intellectual structure of Internet of Things security protocols in the existing literature. Further, in realising this, the study categorised and visualised collected research output documents with respect to annual scientific production, top five sources with the highest number of citations, most relevant authors keywords used and sources. In the interest of countries researcher' profiles involved in security protocols; the analysis also considered top countries with their most prolific affiliations including collaborative work ensured. The findings of this study will be significant and instructive, giving the community and industry additional information and a better understanding of the state of research today and its development trends. The current study can promote new applications, advance Internet of Things security protocols research, and suggest new channels for disseminating knowledge in the area.

The rest of the paper is arranged as follows: In section II, we discuss IoT security protocols. Section III presents the methodology used for data sources and search strategy. Section IV presents a discussion on the results and analysis of search findings. Finally, section V provides a conclusion and recommendations for future work.

II. IOT SECURITY PROTOCOLS

In any data communication network, network security is extremely important as a way of protecting assets in logical and physical manner. In its generic form, network security consists of security services that are capable of allocating access, distribution, monitoring and protecting the underlying assets such as IoT device including their data and software systems [6]. The overall objective is to offer protection by preserving integrity, availability, and confidentiality of system resources. IoT architecture allows a diverse connectivity platforms and technologies such as the Radio-Frequency Identification (RFID), Wireless Sensor Networks (WSN), Machine-to-machine making it more challenging in the provision of reliable and secure solutions [7].

Depending on the nature network topologies, each connected device would work with some protocol such as UDP or TCP. However, it is through these protocols that vulnerabilities can be exploited by threat actors. Although industry experts develop specific protocols to address these vulnerabilities, there are still inadequate in dealing with ever emerging security threats [8]. Examples of specific protocols developed and being used are OS4I, Bluetooth Low Energy (BLE), Zigbee, Z-Wave, Wireless Hart, Sigfox and LoRaWAN. The underlying technological nature of IoT devices may allow security vulnerabilities when performing the following activities [9]:

- Gathering of abundant data – IoT devices and sensors normally collect large scale data, detailed in nature within their environments and users. This data, of which some of it is necessary for their own operation is vulnerable to attacks if not properly secured.
- Connection of virtual and physical environments – A greater impact on attacks is created due to shortened distance created between the virtual and physical systems.
- Creation of complex environments – the complexity and dynamic interactions within the environment in which a single IoT operates increases the attack sur-face.
- Centralisation of architecture – the traditional approach that requires IoT devices and sensors to collect data and send to a base station can have a detrimental effect of security.

Clearly, IoT has become ubiquitous and pervasive within most of our daily lives such as home, cars, hospitals etc. and come with associated security and privacy issues. Despite many efforts such as those by Saleem *et al.* [10] and DDCMS [11], it is interesting to note that there is still lack of standardised security and privacy guidelines for reliable and secure utilisation of IoT systems and services.

III. METHODOLOGY

A. Bibliometric Analysis

Bibliometric analysis is a computer-aided scientific methodology designed to identify essential research outputs or authors and their relationship by checking all publications related to a given topic [12] & [13]. The analysis retrieved provides abundant and relational information about the topic and hence allowing a process of better understanding of the overall background and the status of the topic of interest among other things. The existing literature revealed that there are several bibliometric tools. In this review study, bibliometric analysis was carried out using R Studio on publications related to IoT security protocols field retrieved from Web of Science and Scopus databases. These two named databases were deemed to be suitable tools for improving the search quality in this study because Web of Science (WoS) and Scopus are the two bibliographic databases widely regarded as the most comprehensive databases for various purposes [14]. The outcomes were based on finding evidence of security protocols designed to protect IoT devices from cyber-attacks. Table 1 provides a summary of primary keywords used in the search including the sources utilised in this study to gather all the necessary data.

Table 1. Primary keywords and sources

Primary Keywords	Security AND Protocols IoT AND Devices Cyber-attacks
Sources	Scopus database (accessed on 05 December 2022) Web of Science Database (accessed on 06 December 2022)

As shown in Table 1, the search for published scientific papers was limited to Security Protocols, IoT Devices, and Cyber-

attacks, with no document type restrictions. Two sources were used namely Scopus and the Web Science Databases.

The search rules used to look up papers in Scopus and Web of Science are shown in Table 2 below.

Table 2. Search rules

Database	Search rules
Scopus	TITLE-ABS-KEY ((("Security Protocols" OR "Cybersecurity Protocols") AND ("IoT Devices" OR "Internet of things Devices")) OR (("Cyber-attacks" AND "IoT Devices")))
Web of Science	TS=((("Security Protocols" OR "Cybersecurity Protocols") AND ("IoT Devices" OR "Internet of things Devices")) OR TS=((("Cyber-attacks" AND "IoT Devices"))

Table 3 provides summary results of the search done in December 2022 using the search rules in Table 2.

Table 3. Main information.

Description	Results
Main Information about Data	
Timespan	2016:2022
Sources (Journals, Books, etc.)	488
Documents	774
Annual Growth Rate %	63.21
Document Average Age	1.81
Average citations per doc	7.859
References	23831
Document Contents	
Keywords Plus (ID)	2428
Author's Keywords (DE)	1756
Authors	
Authors	2197
Authors of single-authored docs	33
Authors Collaboration	
Single-authored docs	43
Co-Authors per Doc	3.68
International co-authorships %	16.54
Document Types	
Article	310
Article; book chapter	3
Article; early access	10
Article; proceedings paper	2
Book	1
Book chapter	31
Conference paper	232

Conference review	11
Proceedings paper	156
Review	20

As displayed in Table 3, the period of review study was between 2016 and 2022. The keywords used in the search (see Table 2) resulted in the retrieval of 774 documents from Scopus and Web of Science. The types of documents found in the search include articles, books, book chapters, conference papers, and reviews.

The information obtained from Scopus and Web of science was merged and analysed using R Studio. R is a data manipulation, statistical analysis, and data visualisation programming language [15]. It was used in the study due to its numerous functionalities, which include functions for data retrieval, manipulation, and storage, built-in operators for array and matrix calculations, integrated collection of tools for introductory and intermediate statistical analysis, and many others.

Figure 1 shows the code used in R Studio to merge Web of Science and Scopus data and eliminate all duplicates in order to have accurate data. After the merging, 357 duplicates were removed, resulting in a total of 774 documents.

```

1 library(bibliometrix)
2 library(openxlsx)
3
4 ## importing web of science dataset
5 wos<-convert2df("savedrecs.txt")
6
7 ## importing scopus dataset
8 scopus<-convert2df("scopus.bib",dbsource="scopus",format="bibtex")
9
10 ##combined both datasets
11 combined<-mergebb5ources(wos,scopus,remove.duplicated=T)
12
13 ##exporting file
14 write.xlsx(combined,"All.xlsx")
15
16

```

Fig. 1. R Source code

The results were analysed using Bibliometrix, an R Studio package offering a set of quantitative research tools in bibliometrics and scientometrics [16].

IV. RESEARCH TRENDS ON IOT SECURITY PROTOCOLS

This section presents the results of the bibliometric analysis carried out using R Studio on 774 scientific publications (see Table 3) for the period between 2016 and 2022 related to IoT security protocols field retrieved from Web of Science and Scopus databases.

A. Annual Scientific Production

The annual scientific publications on IoT security protocols from 2016 to 2022 are displayed in Figure 2. As per the data in Figure 2, 774 scientific papers have been published in the past 6 years. With a higher number of publications in the years 2022 (189 publications) and 2021 (178 publications). This is an indication that there has been active ongoing research around the world in the field of IoT security protocols.

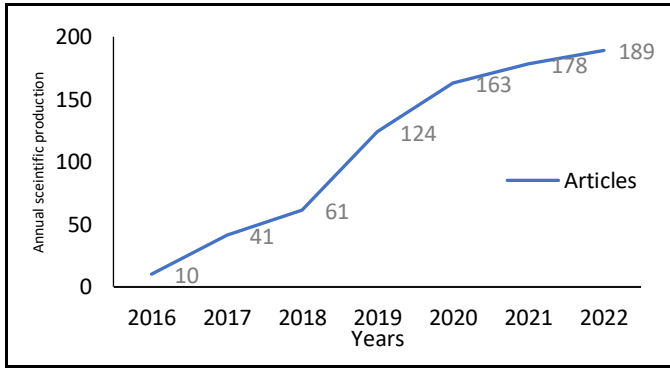


Fig 2. The annual scientific publications on IoT security protocols.

B. The top 5 most cited publications on IoT security protocols.

Further, Table 4 the top five sources with the highest number of citations in the field of IoT security protocols. The classification as shown in Table 4 is based on the number of times a particular published research paper in the field of IoT security protocols has been referred to (or cited) by other researchers.

Table 4. The top five cited publications in the field of IoT security protocols.

Paper	Citations
Sivanathan A, 2019, Ieee T Mobile Comput	164
Diro Aa, 2018, IEEE Commun Mag	148
Sivanathan A, 2017, IEEE Conf Comput	145
Anthi E, 2019, IEEE Internet Things	137
Hussain F, 2020, IEEE Commun Surv Tut	125

Data in Table 4 about the top five cited publications considered in this review were classified in decreasing order (i.e., starting from the most highly cited source to the lower). Based on that the following can be noticed concerning the top 5 cited publications considered in this review:

1. Sivanathan A, 2019, Ieee T Mobile Comput [18] was cited 164 times. The authors address the challenge of the Internet of Things (IoT) being hailed as the next wave revolutionising society, and smart homes, enterprises, and cities are increasingly being equipped with a plethora of IoT devices; in the publication titled "Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics,". They develop a robust framework for IoT device classification using traffic characteristics obtained at the network level.
2. Diro Aa, 2018, IEEE Commun Mag [17] had 148 Citations. The authors of this study, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things

Computing," discuss how the proliferation of smart objects and their diversity, combined with the recent exponential rise in attack frequency and sophistication, have created significant cybersecurity challenges. The study suggests a brand-new distributed deep learning method for fog-to-things computing cyber-attack detection.

3. Sivanathan A, 2017, IEEE Conf Comput [19] was referred to 145 times. In the paper "Characterising and classifying IoT traffic in smart cities and campuses," the study gives smart city and campus operators the ability to find and keep track of their IoT assets based on network behaviour.
4. Anthi E, 2019, IEEE Internet Things [20] had 137 Citations. The paper's working title is "A Supervised Intrusion Detection System for Smart Home IoT Devices." This paper proposes a three-layer intrusion detection system (IDS) that detects a variety of popular network-based cyber-attacks on IoT networks using a supervised approach.
5. Hussain F, 2020, IEEE Commun Surv Tut [21] was cited 125 times. The authors review the security requirements, attack vectors, and current security solutions for IoT networks in this paper titled "Machine Learning in IoT Security: Current Solutions and Future Challenges."

C. The most relevant authors

Various authors have written on the topics of IoT security protocols around the world. Nevertheless, the comparison graphs in Figure 3 only show the top ten relevant authors in the field of IoT security protocols. Referring back to Figure 3, it can be noted that Gharakheili H, Na N, and Sivaraman V have the highest number of publications (11), while the rest of the authors have 6 and 7 respectively.

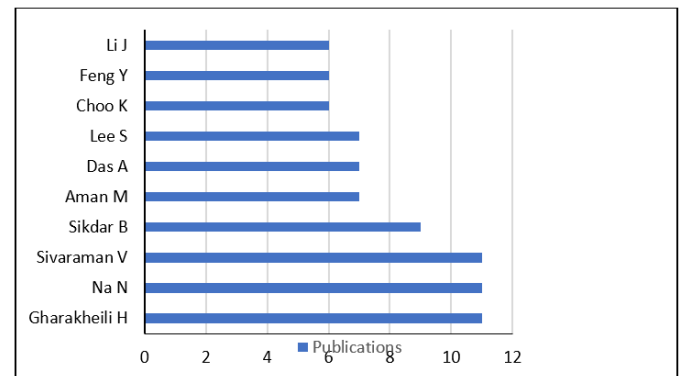


Fig. 3. The most relevant authors in the field of IoT security protocols.

D. The Most Relevant Sources (Publishers).

IoT security protocols research topics have been published by different kinds of publishers, only the top 10 organisations that publish research papers in the field of IoT security protocols were considered in this review. Looking at the data displayed in Figure 4, The IEEE Internet of Things Journal

has the most publications (33), followed by Sensors (28), IEEE Access (24), ACM International Conference Proceeding Series (17), and Lecture Notes in Computer Science (15).

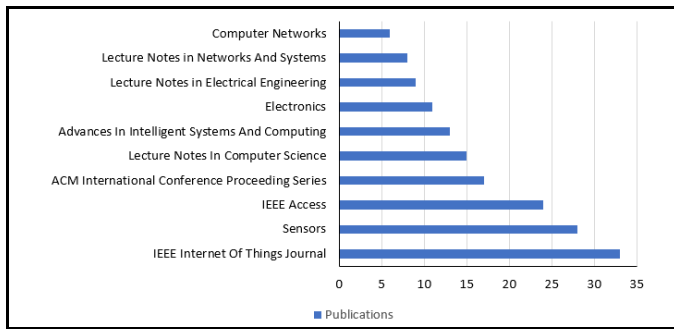


Fig. 4. Most Relevant Sources (Publishers) in the field of IoT security protocols.

E. The top countries.

It is well known that authors from various countries are publishing their research works in the field of IoT security protocols. However, in the context of this study, the emphasis was only on the top 10 leading countries. Furthermore, data about the 10 top countries as shown in Figure 5 was based according to the country affiliation of the first author.

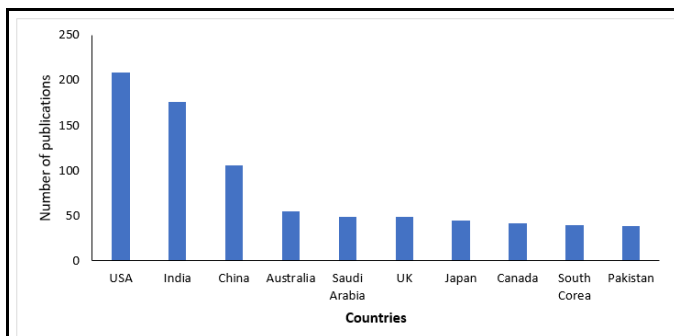


Fig. 5. Top countries contributing to the field of IoT security protocols.

Data as displayed in Figure 5, revealed that the most contributing country in publications to the field of IoT security protocols research is the United States publishing the most papers (209), followed by India with 176 publications, then China, Australia, and Saudi Arabia with 106, 55, and 49 publications, respectively. Based on this data, it can be deduced that at the continental level America and Asia are the top two continents dominating in terms of publications in the field of IoT security protocols. It can be noted that Africa is still lacking behind compared to the two mentioned continents.

F. The most prolific affiliations.

Additionally, in Figure 6 the top 10 most prolific affiliations are presented. This is presented in terms of the number of research papers published by each of these affiliations in the domain of IoT security protocols. The results in Figure 6 indicate that the National University of Singapore and the University of Texas at San Antonio have 10 publications in this field. The majority of affiliations have 5 or more papers

published in this domain. From data patterns in Figure 6, it can be deduced that American and Asian affiliations (institutions) are the dominant contributors in terms of producing research papers in the field of IoT security protocols.

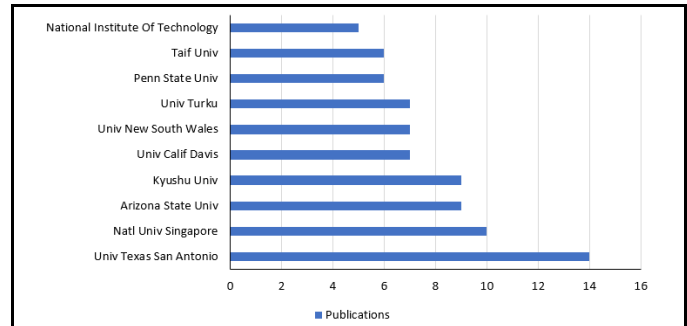


Fig. 6. The most prolific affiliations in the field of IoT security protocols.

G. Country Collaboration Network (Network Analysis)

There have been collaborative efforts amongst authors from different countries in an effort to contribute to the publication of papers in the field of IoT security protocols. Figure 7 illustrates a record of networking circles of collaboration to identify countries that are actively collaborating. Countries belonging in the same cluster have greater collaboration strength. Twenty-four clusters are shown in the country collaboration network in Figure 7. Amongst the 24 clusters, only 10 of them, each having only one country. Furthermore, it is noted that the top contributing countries (see Figure 5) are also the most prominent in the country collaboration network (See Figure 7). The United States of America is the most collaborative country, followed by India, and China. Tunisia is the only collaborative country in Africa that shows collaboration with Saudi Arabia.

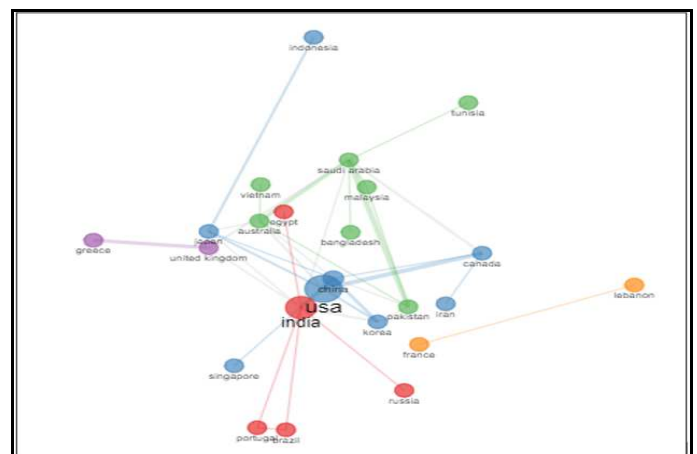


Fig. 7. Country Collaboration Network.

H. Keywords co-occurrence network

Figure 8 illustrates the keywords co-occurrence network with three clusters. A keyword co-occurrence network is about

identifying the appearance of the most frequently used keywords in a document such as a research paper, an article, a book, etc. In other words, it is about checking the number of times the keywords appear in a document during bibliometric analysis. In the context of this review study, a maximum of 50 keywords were extracted from bibliometrix, with 3 as the minimum number of occurrences. Therefore, in this review study, the keywords were separated into 3 clusters and these 3 clusters were further analysed by means of the strength association method.

Cluster 1 (red) has the most keywords related to IoT device security (e.g., authentication, blockchain, network security, public key cryptography), whereas Cluster 2 (blue) has words related to IoT and Data security (Internet of Things, network security, cyber-attacks, cybersecurity, security, security protocols), and Cluster 3 (purple) has keywords related to cyber-attacks (denial-of-service-attack, malware, distributed denial of service). The most common keywords are the internet of things, network security, and cyber-attacks.

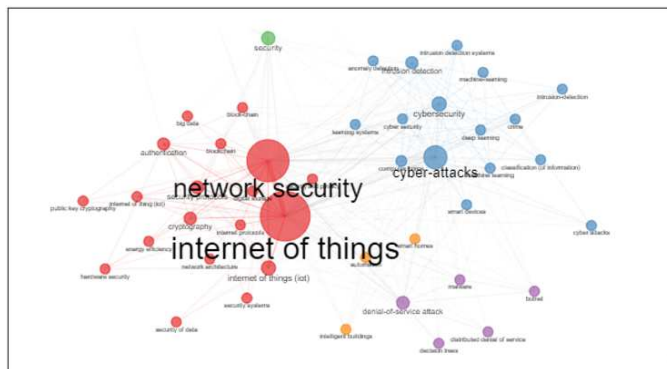


Fig. 8. Keyword Co-occurrence network.

V. CONCLUSIONS AND FUTURE WORK

To better understand the research trends on IoT security protocols, a review study that entailed assessing the status of the existing research in the field of IoT security protocols was conducted. This was achieved through a bibliometric analysis of scientific publications (i.e. articles, books, book chapters, and conference papers) for the period between 2016 and 2022. It emerged that IoT security protocols are an active ongoing research field with American and Asian affiliations (institutions) being the most contributors in terms of producing research papers in this field. In addition, America and Asia are identified to be the top two continents dominating in terms of publications and are the most prominent in the collaboration network. It has also emerged that Africa is still lacking behind compared to the two mentioned continents namely America and Asia. Nevertheless, some kind of effort has been noted from the African continent. For example, the study findings revealed that Tunisia is the only African country with collaborative links based on the topic. It is collaborating with Saudi Arabia.

The results clearly indicate a continued growth in research interest with the most significant in 2022. These results are an indication that research in the field of IoT security protocols is still in its infancy in the African continent compared to other

continents. Hence, African countries still have the opportunity to do more research in the field of IoT security protocols. Therefore, identifying and finding ways to fill these gaps is the main contribution of this paper.

More work is needed in securing IoT systems through continued protocol development including formulation of standardised guidelines that can advance more resilience in securing the operations of the devices.

REFERENCES

- [1] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," *Journal of Computer and Communications*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.
- [2] J. Sen, "Security and Privacy Issues in Cloud Computing," Kolkata, INDIA, 2013.
- [3] Marie Hattar, "IoT's Importance is Growing Rapidly, But Its Security Is Still Weak," Santa Rosa, California, United States, Jan. 2022.
- [4] H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," *J Supercomput*, vol. 76, no. 12, pp. 9493–9532, Dec. 2020, doi: 10.1007/s11227-020-03213-1.
- [5] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015, doi: 10.13052/jcsm2245-1439.414.
- [6] W. Stallings and L. Brown, "COMPUTER SECURITY PRINCIPLES AND PRACTICE Fourth Edition," 2018.
- [7] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *Journal of Sensor and Actuator Networks*, vol. 8, no. 2, MDPI AG, Apr. 22, 2019, doi: 10.3390/jsan8020022.
- [8] J. Tournier *et al.*, "A survey of IoT protocols and their security issues through the lens of a generic IoT stack," *Internet Things, Elsevier*, 2020, doi: 10.1016/j.iot.2020.100264i.
- [9] Trend Micro, "The IoT Attack Surface: Threats and Security Solutions," *Trend Micro*, May 30, 2019, <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions> (accessed Sep. 06, 2022).
- [10] J. Saleem, M. Hammoudeh, U. Raza, B. Adebisi, and R. Ande, "IoT standardisation-Challenges, perspectives and solution," Jun. 2018, doi: 10.1145/3231053.3231103.
- [11] DDCMS, "Code of Practice for Consumer IoT Security," UK, 2018, [Online]. Available: <https://www.gov.uk/government/publications/secure-by-design>
- [12] Nicola. de Bellis, *Bibliometrics and Citation Analysis: From the Science Citation Index to Cybermetrics*. Lanham (Md.): Scarecrow Press, 2009.
- [13] D. Hicks, P. Wouters, L. Waltman, S. de Rijcke, and I. Rafols, "Bibliometrics: The Leiden Manifesto for research metrics," *Nature*, vol. 520, no. 7548, Nature Publishing Group, pp. 429–431, Apr. 23, 2015, doi: 10.1038/520429a.
- [14] R. Prancutè, "Web of science (Wos) and scopus: The titans of bibliographic information in today's academic world," *Publications*, vol. 9, no. 1, MDPI AG, Mar. 01, 2021, doi: 10.3390/publications9010012.
- [15] V. Krotov, "A Quick Introduction to R and RStudio® Tutorial," 2017, [Online]. Available: <https://cran.r-project.org/>
- [16] M. Aria and C. Cuccurullo, "bibliometrix: An R-tool for comprehensive science mapping analysis," *J Informetr*, vol. 11, no. 4, pp. 959–975, Nov. 2017, doi: 10.1016/j.joi.2017.08.007.
- [17] A. Abeshu and N. Chilamkurti, "Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 169–175, Feb. 2018, doi: 10.1109/MCOM.2018.1700332.
- [18] A. Sivanathan *et al.*, "Classifying IoT Devices in Smart Environments Using Network Traffic Characteristics," *IEEE Trans Mob Comput*, vol. 18, no. 8, pp. 1745–1759, Aug. 2019, doi: 10.1109/TMC.2018.2866249.
- [19] A. Sivanathan *et al.*, "Characterizing and classifying IoT traffic in smart cities and campuses," *2017 IEEE Conference on Computer*

- Communications Workshops, INFOCOM WKSHPS 2017*, pp. 559–564, Nov. 2017, doi: 10.1109/INFCOMW.2017.8116438.
- [20] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, “A Supervised Intrusion Detection System for Smart Home IoT Devices,” *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, doi: 10.1109/JIOT.2019.2926365.
- [21] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1686–1721, Jul. 2020, doi: 10.1109/COMST.2020.2986444.



Dr Gardner Mwansa Ph.D.

Gardner Mwansa received a Bachelor of Science degree in Pure Mathematics and Computer Science from University of Zambia. He further obtained a master's degree in Information Technology and a Doctor of Philosophy from University of Namibia and University of South Africa respectively. He has industry and academic experience in various positions and currently a Senior Lecturer at Walter Sisulu University. His research interest is within the scope Ntima Mabanza bordering emerging technologies, cybersecurity, and cloud-based software systems.



Dr Ntima Mabanza Ph.D.

Ntima Mabanza obtained his Ph.D. in Computer Information Systems from the University of the Free State (UFS) in South Africa. Currently, he is a Senior Lecturer at the Department of Information Technology, Central University of Technology Free State (CUT), Bloemfontein, Free State, South Africa. His research interests include Pedagogical Interface Agents, Human-Computer Interaction, User Experience, Usability Testing, and Bibliometric Analysis