Journal of Theoretical and Applied Information Technology
31st January 2022. Vol.100. No 2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SYSTEMATIC REVIEW ON THE CHALLENGES OF ADOPTING ADVANCED SECURITY SOLUTIONS ONTO IOT-BASED SMART DEVICES

MATHURI GURUNATHAN[1], MOAMIN A. MAHMOUD[2], MOHAMMED NAJAH MAHDI[3]
[1]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia
[2]The Institute of Informatics and Computing in Energy (IICE), Universiti Tenaga Nasional, Malaysia
E-mail: [1]mathuri_maths@yahoo.com, [2]moamin@uniten.edu.my, [3]najah.mahdi@uniten.edu.my

ABSTRACT

Recently, the Internet of Things (IoT) has been one of the most active research topics in Smart Applications that attracting much attention from both researchers and developers. IoT aims to connect billions of things by sharing and receiving information using Internet Protocol (IP) that enables IoT devices to store and access online data. However, despite the benefits of IoT in smart applications, security threats are expected to be increased substantially. Security in IoT is one of the most noteworthy challenges in the interconnected world. The Internet of Things will be profoundly joined in our lives now and more in our future, therefore, it is important to venture up and pay attention to cyber threats seriously. Although the increasing number of publications in the area of IoT devices security in smart applications, there still are limitations in the comprehensive literature review. To provide a clear insight into this limitation and support researchers, we need to understand the current state of research in this area. Consequently, this study presents a review of articles published from 2010 to 2019 on IoT devices security in smart applications. A manual search is used to ensure the retrieval of all relevant studies. The final 60 selected papers are reviewed and relevant information extracted based on a set of research questions. The review aims to altogether examine the observational on validating IoT security devices protocol development.

Keywords: *IoT; Smart Devices; Security And Privacy; Systematic Review.*

1. INTRODUCTION

Smart is a domain, where various devices are networked together to give better services in a universal way to the people. Hence, such devices will have smart capacities to gather, examine and indeed make choices without any human interaction. On the other hand, the Internet of Things (IoT) plays a vital source in converting things into smart, such as smart homes, smart grids, smart cities, smart agriculture. It could be described as a huge network that interfaces devices and let those devices communicate with one another over the internet [1]. All of the connected devices accumulate and share information around how they are utilized and the situations in which they are worked [2]. According to IoT analytics statistics, as of the year 2018, they were 7 billion IoT devices were connected to the internet. By the year 2020, it is expected to reach 10 billion devices [3]. The outcome is an interconnected smart world, where people and devices connect, building up a smart environment in which sharing and exchange data services is continuous [4].

The usage of technology in our daily lives increases day by day. As new technology develops, more governments, businesses, educations, and each individual embraces and depends on these devices for an everyday process, new security concerns may arise with a higher percentage [5]. For example, somebody might install IoT applications but does not figure out the poor security of the devices that have been vulnerable and has the potential to be seen by others [6]. Unlike poor security, people too must consider the data security of each IoT device. Kouicem [7] states, “IoT suffers from few security issues, which are more challenging than those from other areas regarding resources-constrained IoT devices. In this situation, security speaks to a vital perspective to be tended to, due to the abnormal state of heterogeneity of the involved IoT devices and the security issues that exist nowadays for IoT. It is not easy to address difficulties even with the significant

measure of existing work that has been accomplished for a considerable length of time in the zone of security and privacy.

The article is organized as follows: Section 2 depicts the research process in detail. Section 3 shows the review results including distribution results and the graph of the results. Section 4 covers motivation, challenges, and recommendations in the study of review. Section 5 discusses the findings based on the review which is the main discussion in Section 4. The summary of our contributions as well as a discussion and the conclusion of the study are discussed in Section 6.

2. RESEARCH SELECTION METHOD

To accomplish the target of answering the research questions, we conducted the SLR in agreement with the direction distributed by Kitchenham and charters [8]. Figure 1 illustrates the SLR process.

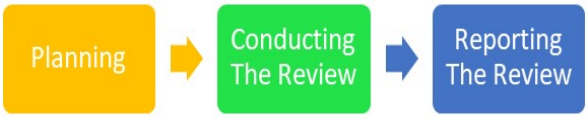

Figure 1: SLR Process

2.1 The Research Question

As indicated by [8], SLR is an evaluation and interpretation of all current research that is important to a particular research question. Specifying the research question is the most significant piece of any systematic review. It is at that point necessary to indicate the research question, which is the foremost critical portion of any SLR. The review questions drive the complete systematic review methodology.

Table 1: Research Question.

ID	RESEARCH QUESTION	MOTIVATION
RQ1	What are the most used security protocols for IoT?	Identify the most used security protocol for IoT?
RQ2	What are the IoT applications involved in security issues?	Identify the IoT applications involved in security issues?
RQ3	What are the challenges in IoT security devices?	Identify the IoT security devices related challenges?

2.2 *Planning the Review*

In this phase, a review protocol shows the techniques that will be utilized to embrace a specific systematic review. The review aims to altogether examine the observational on validating IoT security devices protocol development. The methodology that will be utilized to look for primary studies will include search terms and resources to be looked at. Resources include specific journals, digital libraries, and conference papers.

2.3 *Eligibility criteria*

These categories were gotten from a pre-study of the literature without limitations. Three screening and filtering iterations, the articles that are not eligible based on the desired criteria were avoided after the first round. The criteria of exclusion included (i) non-IoT-based articles, and (ii) non-English articles.

2.4 *Identify Relevant Research and Primary Studies*

The overall query search for this research is 679 articles as per the following: 252 articles from ScienceDirect, 322 articles from IEEE Xplore, and 105 articles from Springer. The filtration process has been made twice according to the sequence embraced in this research phase. A sum of 45 articles out of 679 articles were duplicates and hence removed and 634 articles were remaining. After reviewing the titles with abstracts, 322 articles were removed, leaving 312 articles. Besides, removing 124 articles after the full-text review, the balance of 188 articles remains with IoT-based security devices. Last but not least, the last full-text review removed 105 of the 188 articles, leaving 60 articles for the last set. The rest of the articles were identified with IoT security devices articles through various subjects.

2.5 Data Extraction

From using data extraction, we extracted important information provided by the primary studies. We extracted vital data information given by the primary studies. Every question is the data extraction form. We removed significant data given by the primary studies utilizing the data extraction form. In Figure 2 demonstrates the quantity of the papers chose at each phase of the process and the attrition rate of papers got from first keyword searches on every stage down to the last determination of primary studies.

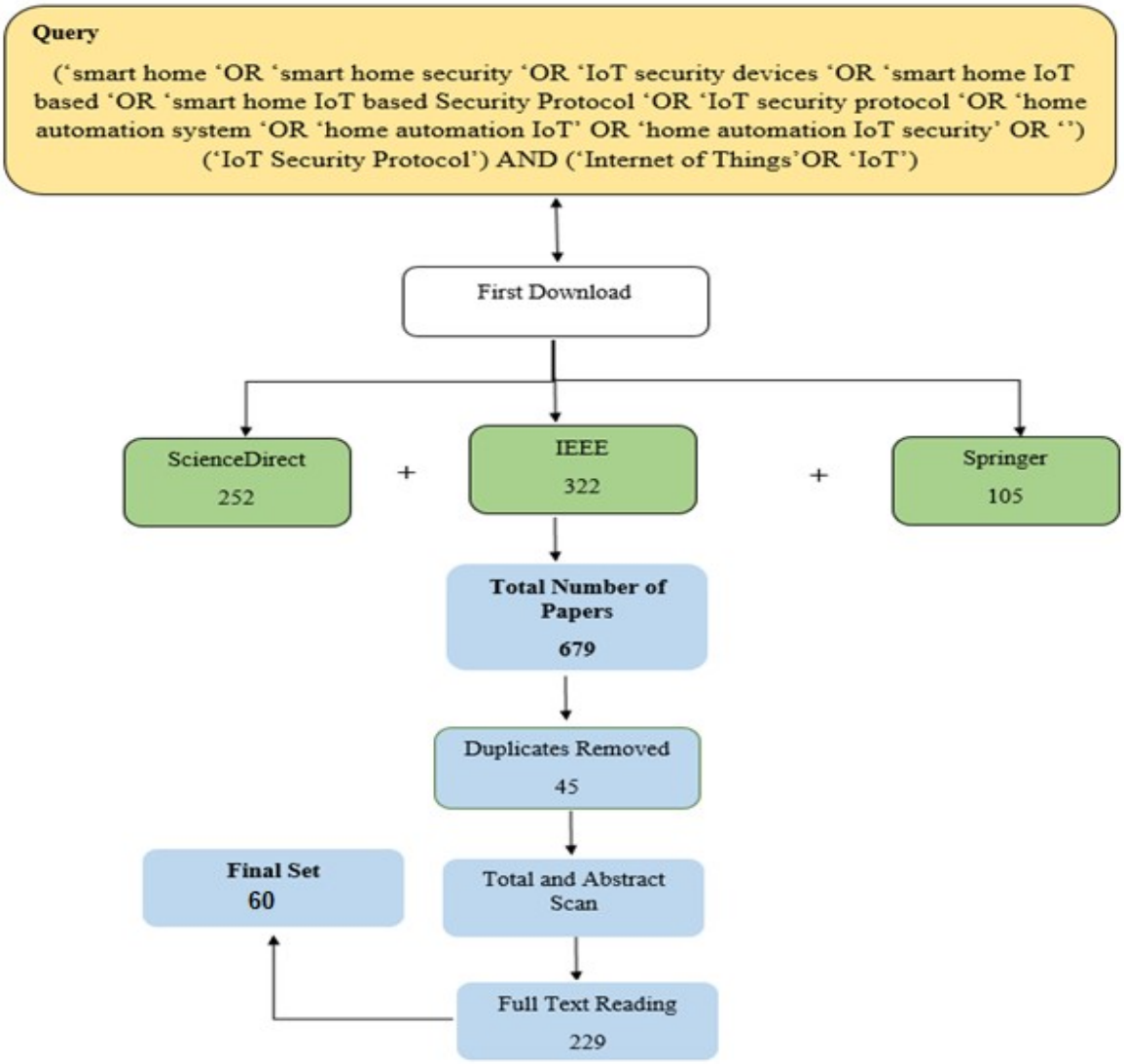

Figure 2: Attrition of papers through processing

2.6 Reporting the Review

The data separated from 60 primary studies were utilized to formulate answers to the three research questions. We intently followed the guidelines given by Kitchenham [9] in setting up the SLR. The review protocol of this study is outlined in Figure 3.

3. REVIEW RESULTS

In this segment, we present the blend of proof of our SLR, beginning with the analysis of the literature. Figure 4 demonstrates that the three databases store various research articles and Figure 5 demonstrates the publication period from the year 2010 to 2019.

3.1 RQ1: What are the most used security protocol for IoT?

Security is probably the greatest worry in IoT application, its development pulled in numerous investors to extend into utilizing and managing information with various levels of privacy, with highly personal data from the public [10] [11]. Blockchain at its core cryptographically secured, distributed ledger that permits for the secure exchange of information between parties [12]. Hence, blockchain technology serves as a strong solution to improve and brace information security in different ways [13]. Traditionally IoT systems are subordinate to centralized engineering.

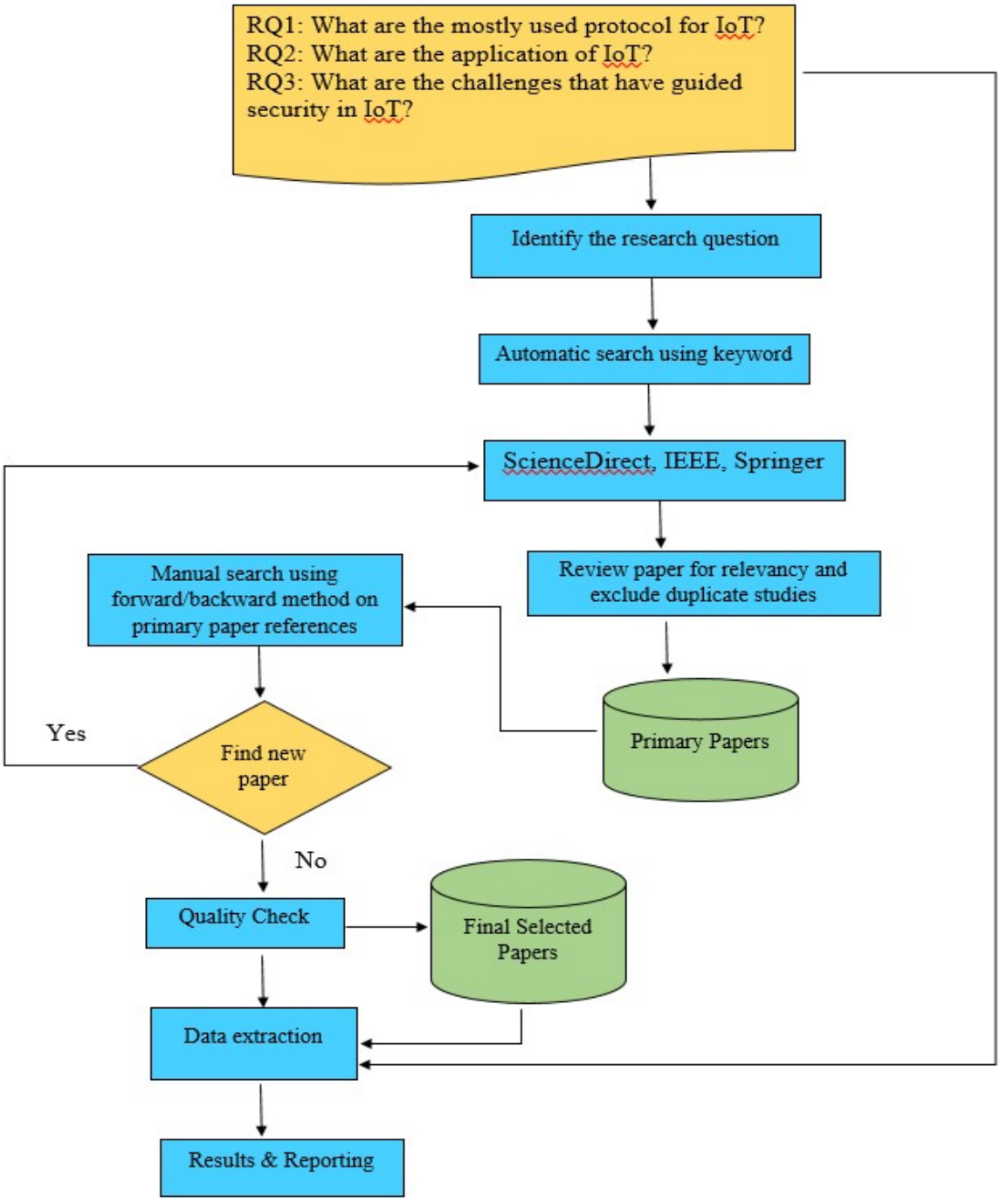

Figure 3: The review protocol

Data is sent from the IoT devices to the cloud where the information is handled utilizing analytics and after that sent back to the IoT devices [14]. Billions of IoT devices are set to connect to IoT systems within the coming years, this sort of centralized system has exceptionally limited scalability, uncovered billions of weak points that compromise network security, and will be gotten to be fantastically costly and slow on the off chance that third parties have to always check and verify each and each micro-transaction between IoT devices [13].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

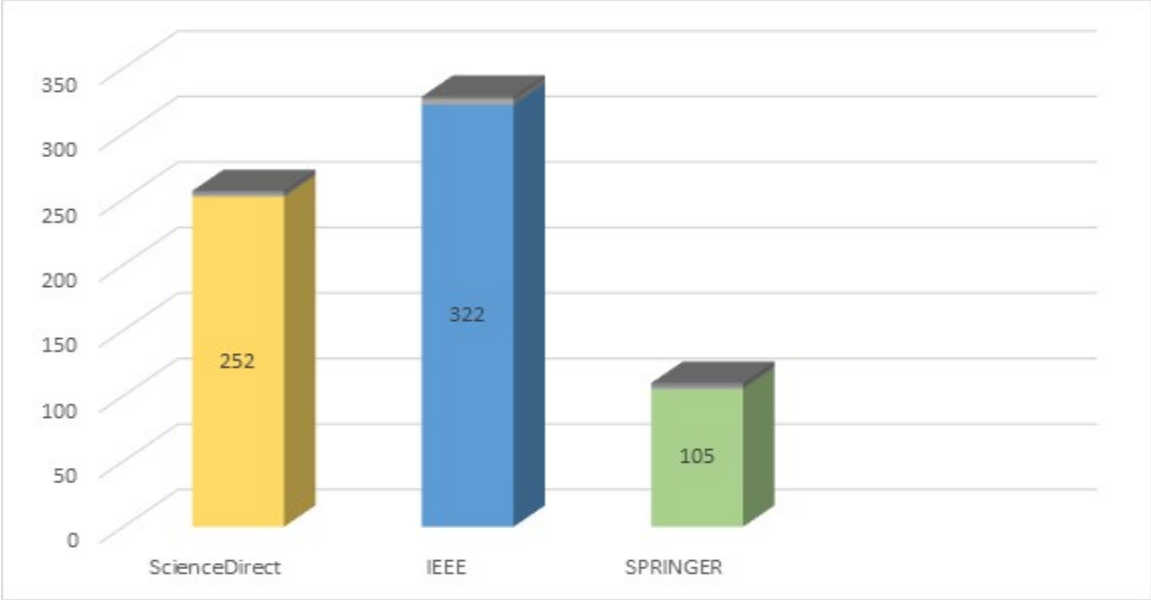

Figure 4: Journals from three different database

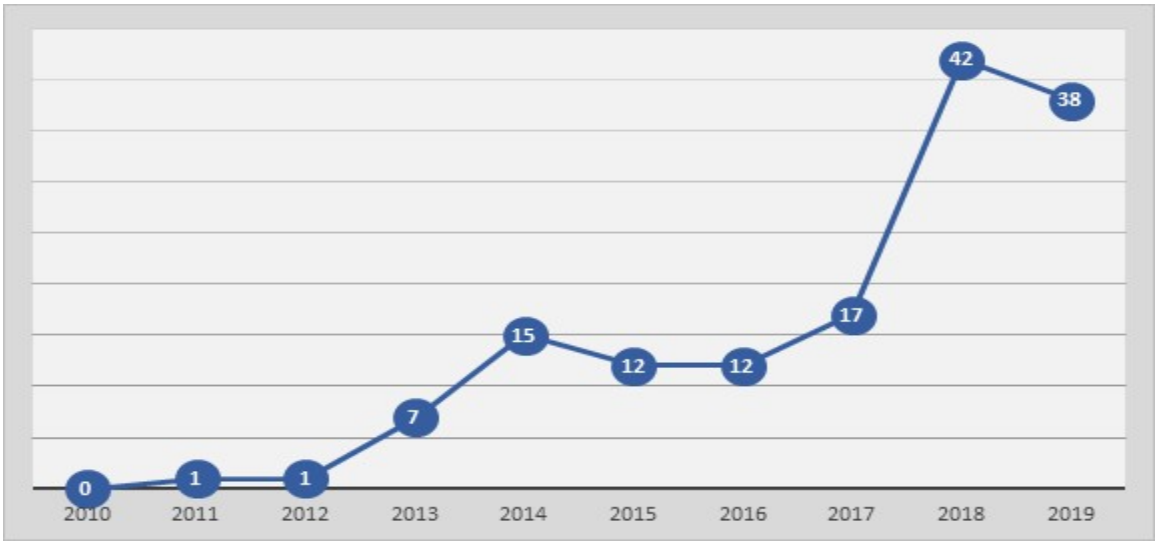

Figure 5: Publication Period of Smart Home IoT Devices Protocol

Blockchain technology will allow devices to operate safely and independently by making agreements that are just endless completion of particular requirements. There will be no trusted third party controlling the ledger and it has no central authority for the network. Blockchain is a decentralized network that is immutable and it carries no transaction fees [15]. Besides, data is shared over a decentralized, cryptographically secured network, which means it turns out to be hard to compromise the system security. Table 2 below shows the benefits of blockchain technology

MQTT is one of the foremost commonly utilized protocols in IoT projects. It stands for Message Queuing Telemetry Transport. This protocol is a message-based protocol, amazingly lightweight and for this reason, it is received in IoT. Nearly all IoT platforms encourage MQTT to send and get information from smart objects. Hence, there are a few usages for different IoT boards like Arduino, Raspberry, and so on and there are other IoT protocols utilized to execute IoT projects but MQTT is one of the foremost effective [16].

Table 2: Features Of MQTT

Security	Despite the fact that MQTT messaging utilizes an unbound TCP, we can almost certainly encrypt information with TLS/SSL Internet security to create it vigorously, when actualizing for the mission-critical business [19]. Ready to have fractional and total encryption based on the resourcefulness of the network and security order.
Central Broker	We might get billions of gadgets on the Internet throughout the following 5 to 10 years. An intermediary which can go about as a server can adequately decrease the number of bundles that fall into the web and the measure of preparing the individual memory required for the customers. We ought to have the option to construct a network of profoundly interoperable intermediaries crosswise over various sellers
Last WILL & Retained Message	a. Final WILL makes a difference in knowing whether the specific client is accessible or not. It isn't worth holding up for something that won't happen. The audience members can be put on the power saver mode with interim-based wake-up to check the publisher's accessibility. b. Held messages will offer assistance endorsers get messages that were distributed a few times sometime recently. These messages exceedingly decouple both the publisher and the subscriber to work free of each device. [20]

Subsequently, MQTT has an amazing little footprint and negligible bandwidth, which makes it very helpful for IoT applications. MQTT could be a publish-subscribe-based messaging protocol, very basic and lightweight. It is an application layer convention that takes a shot at top of the TCP/IP stack.

The most thoughts of its plan are to decrease the network bandwidth just as device resource requirements, endeavoring simultaneously to give reliability and a few levels of delivery guarantee [17]. MQTT information isn't encrypted so it is to be sure an issue in a wide range of situations. It does not make a difference if the broker uses an authentication component or not since the information in travel can effortlessly be sniffed by an attacker [18]. This issue is once more a privacy one meaning that information can be seen by anybody with fundamental networking skills.

Machine-to-Machine (M2M) communications is a developing communication worldview that gives ubiquitous network connectivity between devices besides a capacity to communicate independently requiring no human mediation [21]. IoT speaks to a future where billions of day-by-day objects and encompassing situations will be associated and overseen through a range of communication systems and cloud-based servers [22]. Showcase estimate projections appear to have a huge potential for an M2M showcase that's expected to grow quickly within a few long time. Besides, this is often due to several factors counting the widespread availability of wireless advances, declining costs of M2M modules, and financial motivating forces.

Eventually, Machine to machine will be included in all objects, including television, vehicles, and smart appliances and there is a huge amount of data is a security risk [23]. The information collected is put away in an unknown location in the cloud and can disclose data about individuals, such as buying a design, locations, communication activities, and indeed health data. Therefore, M2M devices are unsupervised and set in a variety of locations, which makes hackers access to each of the devices and exposes them to theft, reuse, and extortion). As the M2M advertise develops, analysts expect that the number of false uses of these devices will develop [24].

Simultaneously, in any case, M2M presents the methods by which extra difficulties may happen. Issues of security, which is simply the capacity of the system to stay alright for users and associations, and of client control, which is a user can have control over the user's very own character and experience, are yet to be settled [25]. Lastly, Table 3 shows the features of the machine to machine communications.

Table 4 below will be the comparison between HTTP and CoAP.

Table 3: Machine To Machine (M2M) Features

Multitude	It is expected that the quantity of connected IoT devices in an M2M ecosystem will before long surpass the whole of all those that straightforwardly connected with people (Like example: Mobile phones, Laptop, tablets, etc.) An increased order of size within the number of devices will generate enormous transmissions, coming about in scalability issues for existing systems [26]
Less Data Transmission	Most M2M devices create little bursts of natural traffic which may have periodic patterns. Thus, the system must most likely help little measures of information with insignificant effect
Energy Constrained	Mainly, M2M devices are battery worked and regularly conveyed in zones where continuous human access and battery substitution aren't effectively conceivable [27]. In this way, energy proficiency for M2M communication turns out to be significant to delay network lifetime.
Security Vulnerabilities	The higher the number of connected devices in the coming years, the higher will be the target for hackers, and security concerns will be a huge impact. [25]

Table 4: Comparison Between HTTP And Coap

CoAP	HTTP
UDP	TCP
Using IPV6	Using an IP layer
CoAP will be using both client-server and public models	HTTP will be using client and server architecture
Less overhead and CoAP will be always simple	More overhead than CoAP and its complex

Figure 6 and Figure 7 shows data collections charts from the year 2010 till 2019.

3.2 RQ2: What are the IoT applications involved in security issues?

One of the foremost touted advantages of home automation is giving peace of mind to house owners, enabling them to monitor their homes remotely, countering threats such as a forgotten coffee maker left on or house door left open. Besides, a smart home moreover helps consumers improve proficiency [28]. Rather than leaving the air conditioning on all day, a smart home system can get familiar with your behaviors and ensure the house is chilled off when you arrive home from work [29]. In some way, the devices expose to a huge number of attacks and make them vulnerable. Authentication is required to ensure security and identify characters to prevent attackers and malicious attacks [30]. IoT is viewed as a constrained resource environment where handling and energy resources are limited. A lightweight authentication approach with vigorous security highlights is required to protect energy and fit processing capabilities [31]. Figure 8 shows a comparison of the IoT applications percentage up to the present and Figure 9 shows number of security vulnerabilities from 2010 – 2018.

3.3 RQ3: What are the challenges in IoT security devices?

Manage testing and update devices: The vast majority of these devices and IoT items don't get enough updates whereas, few don't get updates at all [32]. This implies devices that were once thought of as secure when the clients originally got them to end up insecure and in the long run prone to attackers and other security issues [33]. Brute Force Attack: When users still use the default passwords of a device for a very long time, their private information will be at very high risk [34]. Brute force is all about guessing the password and the default password will be the easy way for the hackers to identify. Secure Communication: Utilizing separate networks to isolate devices moreover makes a difference with building up secure, private communication, so that information transmitted remains confidential [35]. Data security and privacy: Rules should be set to redact and anonymize sensitive information before putting away and disassociating IoT information payloads from data that can be utilized to recognize us [36]. Authentication: IoT devices must establish their identity sometime recently they can access gateways and upstream services and applications [37] [38]. Hence, two-factor authentication (2FA) will be a strong authentication and have better security [39].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

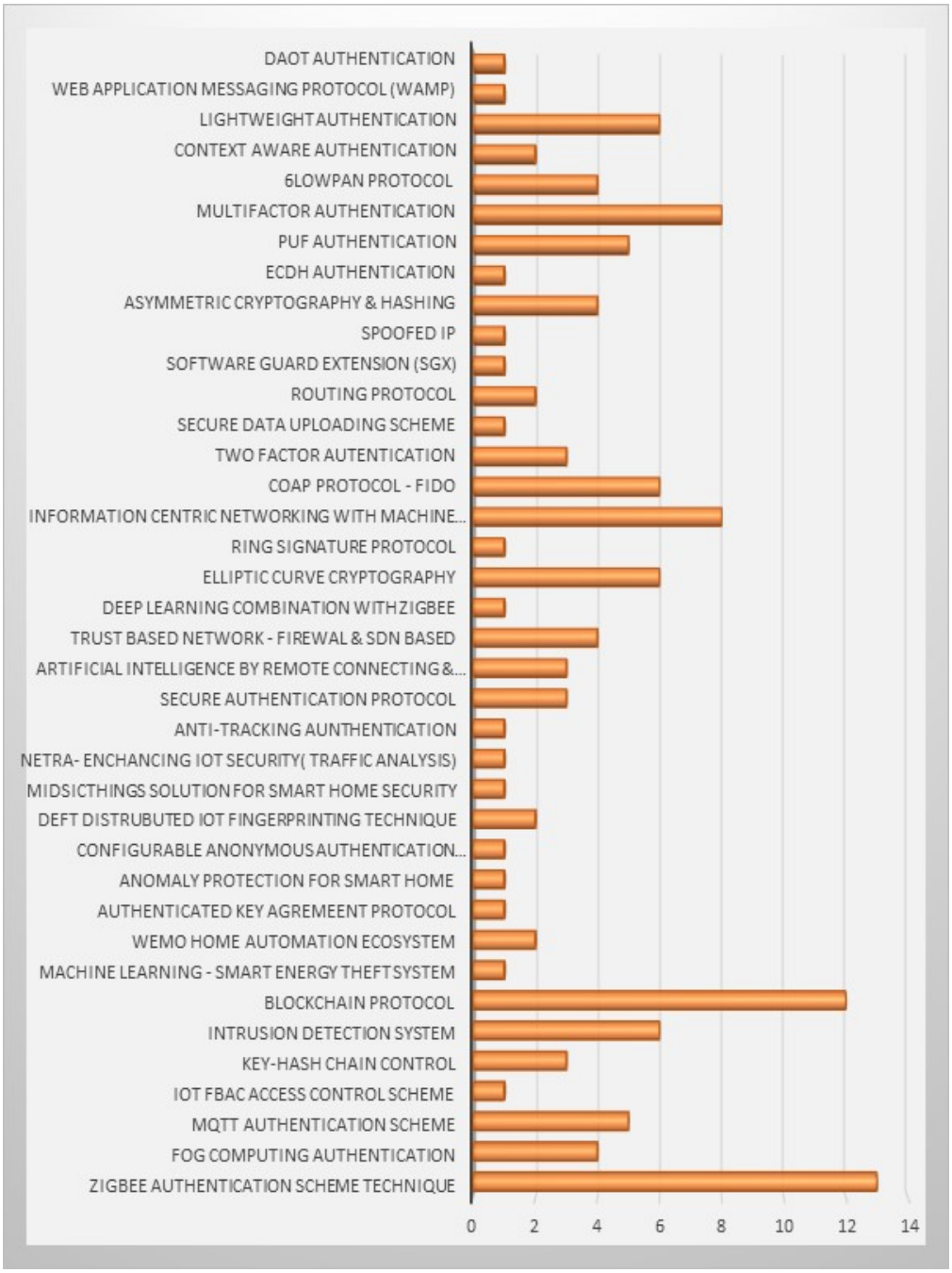

Figure 6: Number of articles from 2010-2019

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

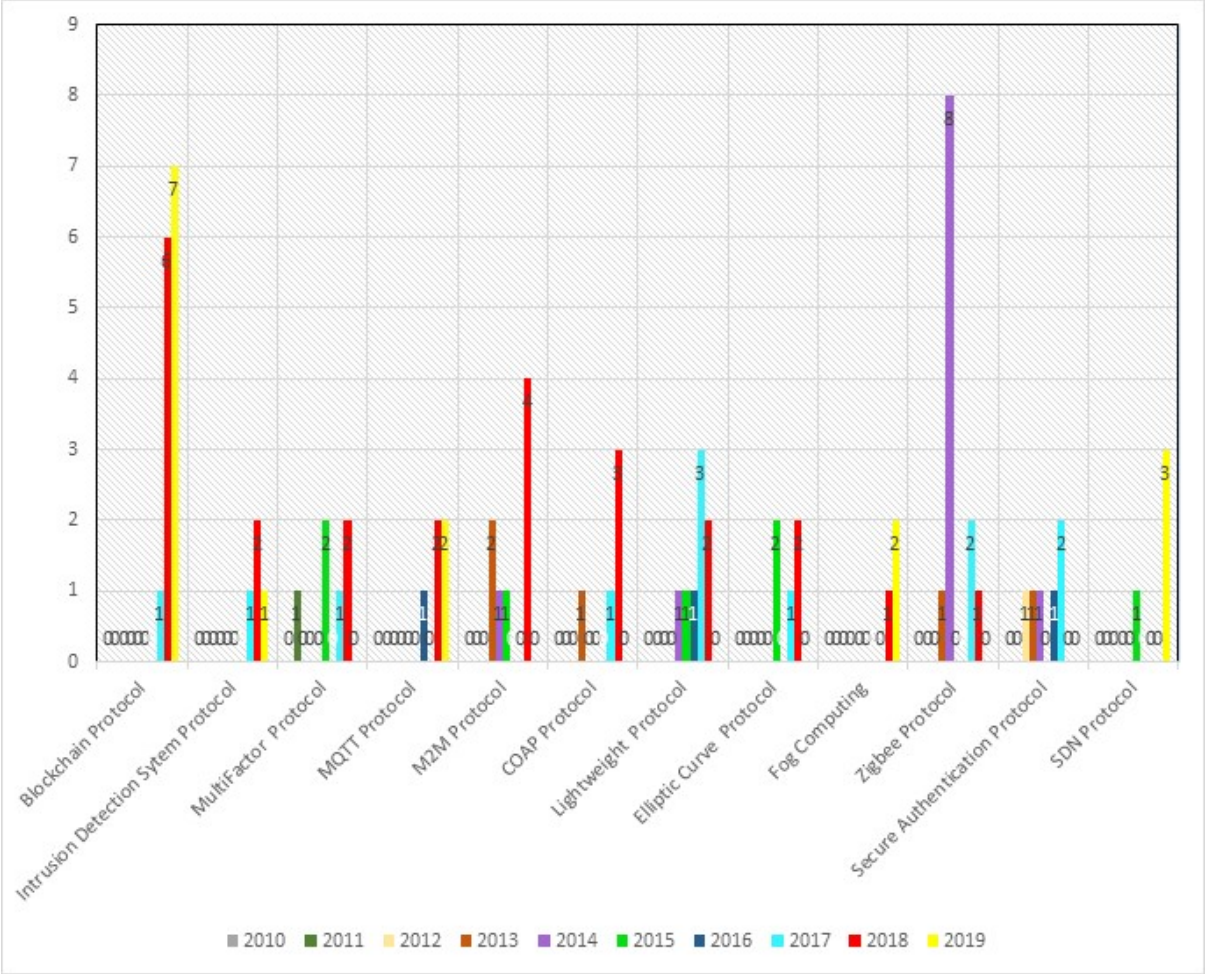

Figure 7: Top highest number of protocols from 2010 to 2019

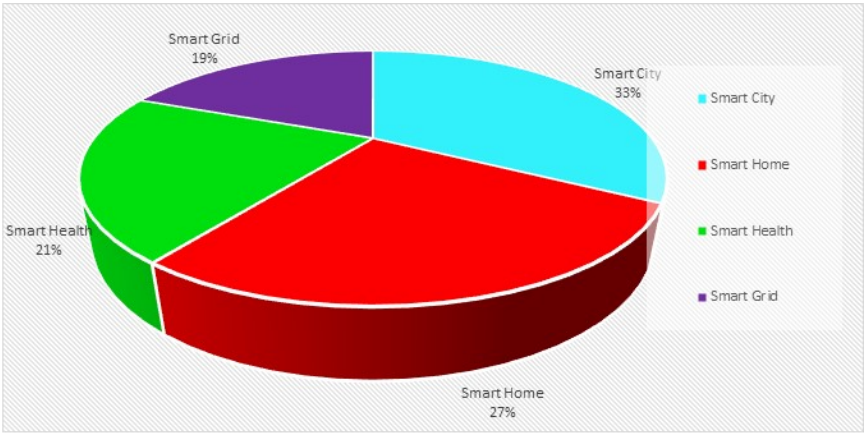

Figure 8: Percentage of the showed IoT Applications.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

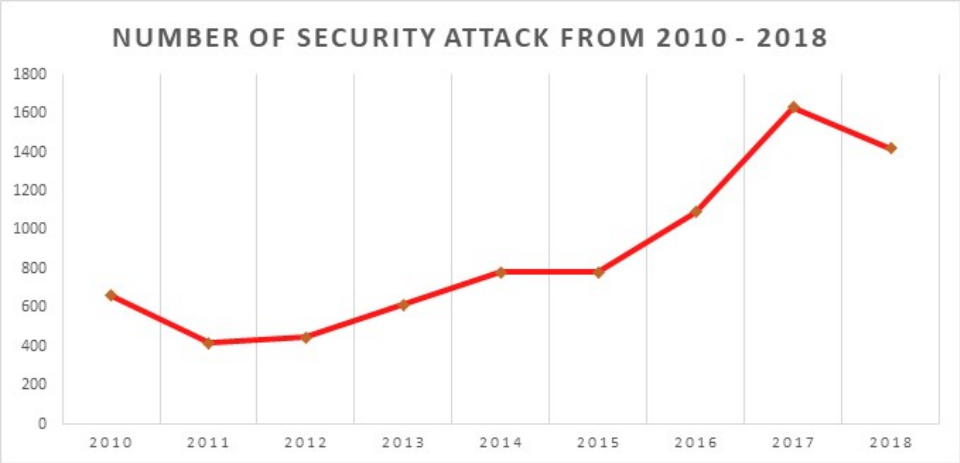

Figure 9: Number of Security Vulnerabilities from 2010 – 2018

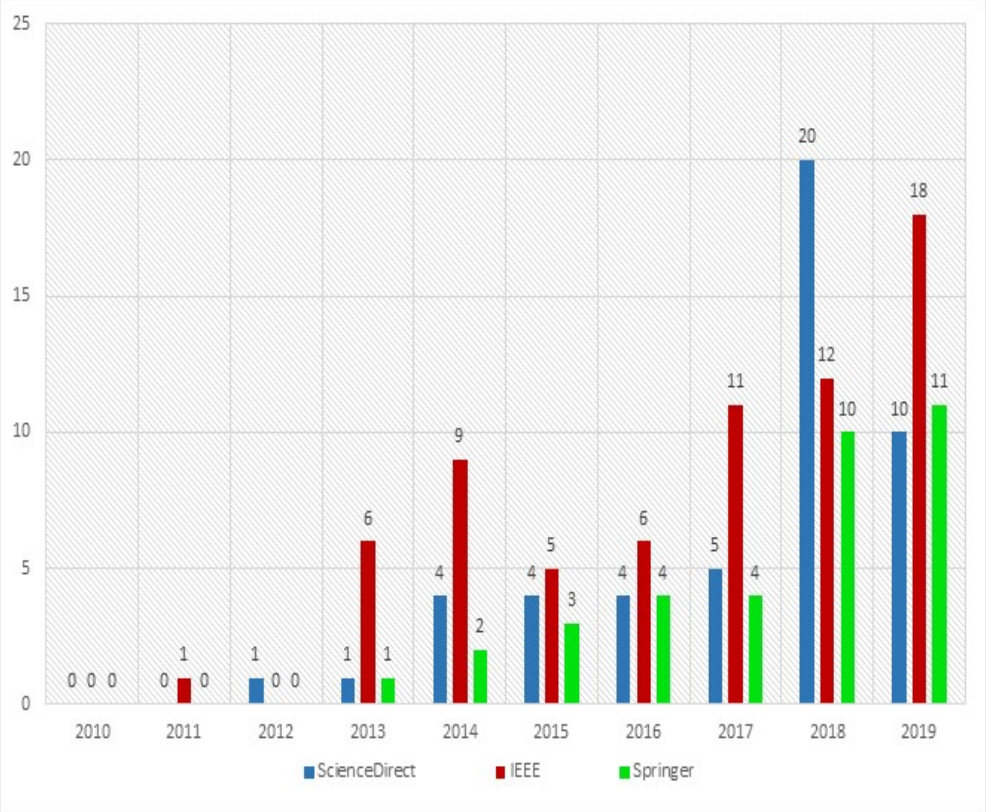

Figure 10: Distribution of research papers by publisher

3.4 Distribution results

Figure 10 appears that the three databases store various research works. The distribution of scholarly papers from 2010 to 2019 is shown.

3.5 Distribution by authors' nationality

Figure 11 presents the articles on the security protocol of IoT devices in a smart system.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

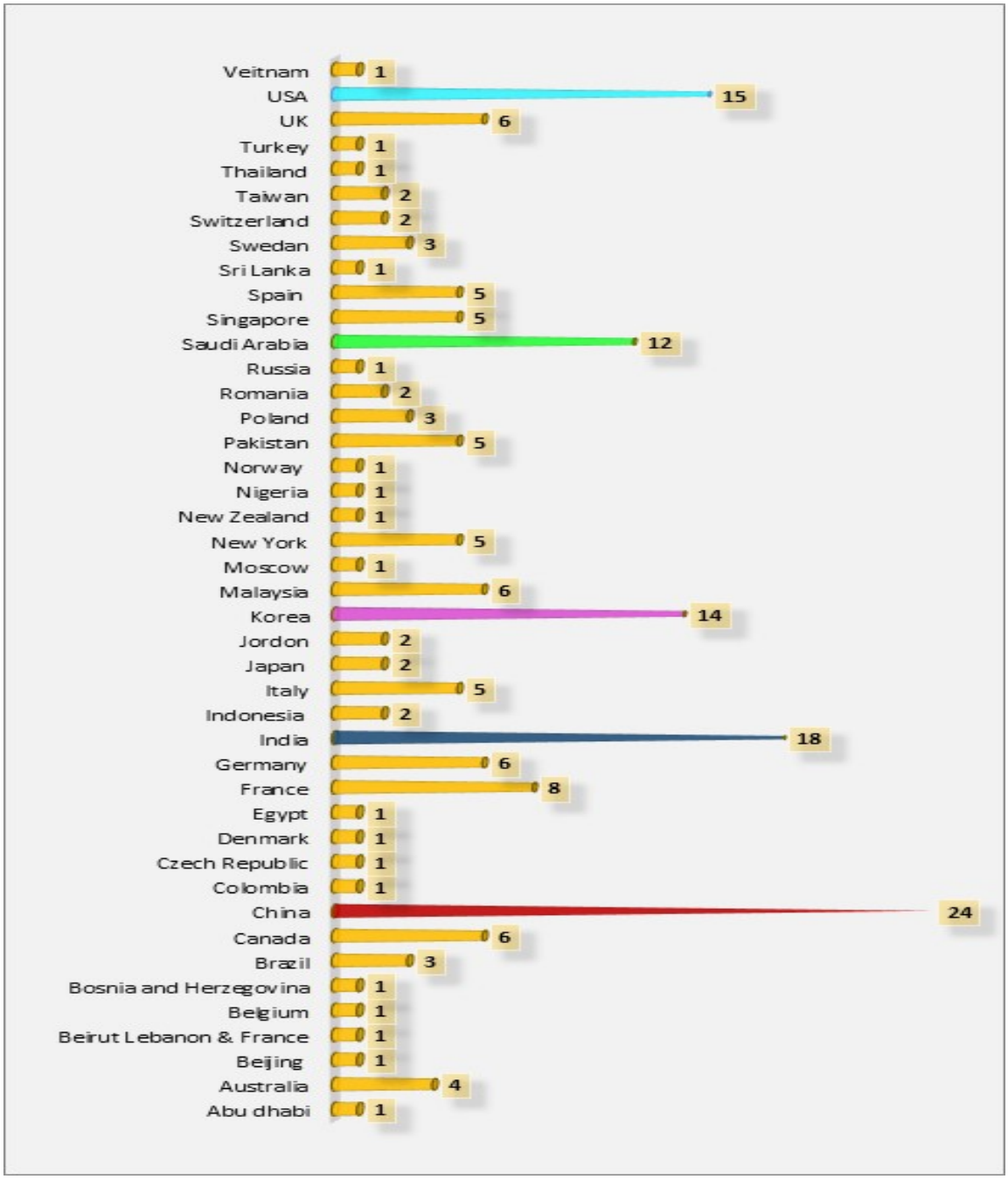

Figure 11: Distribution by authors' nationality.

4. MOTIVATIONS

The advantages are enormous, however not without risk. Remote, smart monitoring and control for processing plants, smart homes, smart cities, furthermore, transport can build effectiveness and security. Yet these useful tools can be misused by attackers. However, the advantages of utilizing security for IoT devices based on smart things are evident compelling. This segment exhibits a few of the advantages reported within the literature, which are assembled into categories relying upon comparative advantages, as appeared in the diagram below [40] [41] [42] [43]. Figure 12 summarises the motivation related home automation, healthcare, energy, and entertainment.

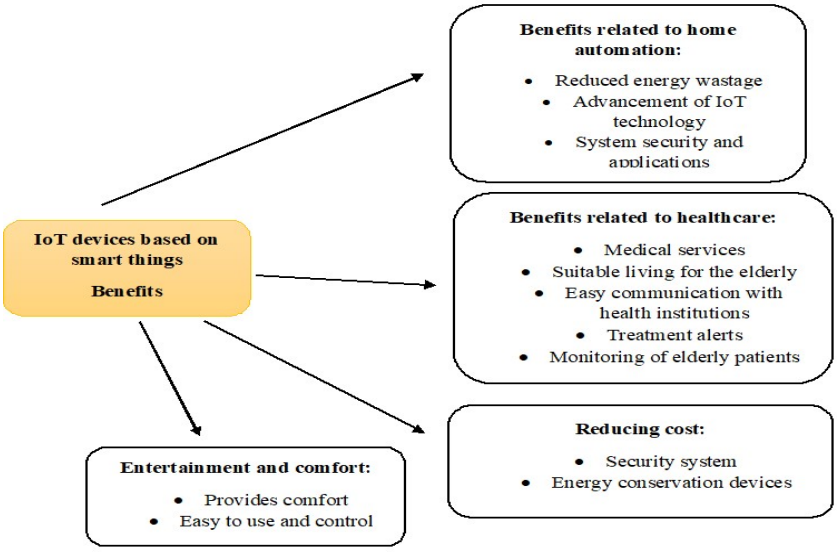

Figure 12: The motivations of IoT devices based smart things

4.1 Challenges

As IoT takes control over the world, numerous security challenges identified with IoT organizations within the consumer and enterprise space are becoming known. The more devices get connected with the web, the more intricate the IoT environment moves toward becoming, and the more sensitive data is at risk [44] [45] [46] [47]. Figure 13 summarises the challenges identified in this study.

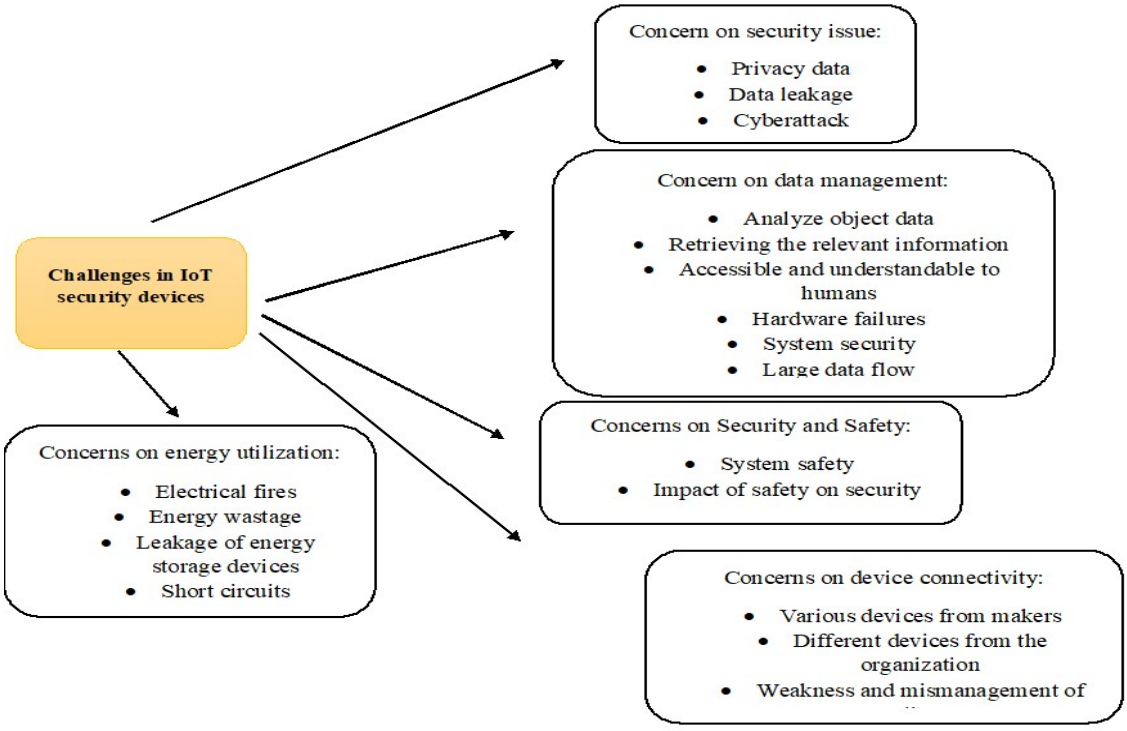

Figure 13 Summary of challenges

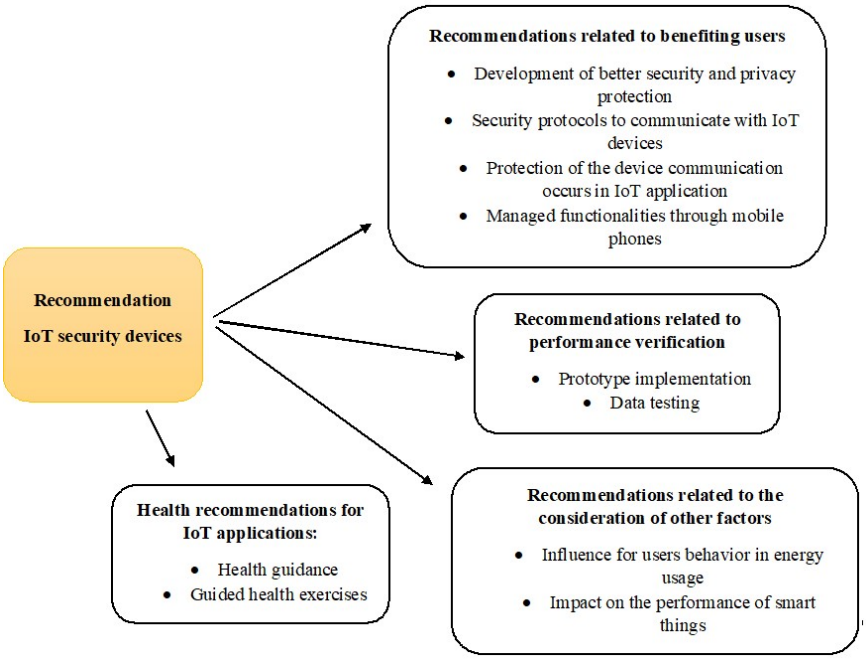

Figure 14 Suggested recommendations

4.2 Recommendation

Recently, devices with not exactly attractive security states were taken over by massive botnets consisting of a huge number of devices that had the option to launch a noteworthy DDoS attack that crippled a few online services. Security must be a top need in the strategy of producers and not a bit of hindsight. Consumers are needing arrangements built-in view of security and which ensures their homes, their lives, and their private data. There is a requirement for better guidelines because of a lack of product certifications marks to help consumers in separating brands and items as for their security state. To beat the challenges, the analysts have recommended potential future works [46] [48] [49]. Figure 14 summarises the recommendations suggested in this study.

5. FINDINGS

The findings have shown the accompanying three research questions of this study:

5.1 What are the most used protocols for IoT security?

An example of IoT protocols [50] that are being used for security is M2M, Blockchain technology, Zigbee, SDN, CoAP, etc. The IoT Protocols is such a framework that will transfer information on the internet. Be that as it may, it will transfer information at exactly that point when the communication network between the two connected devices is protected [51]. General protocols are used for PCs, mobile phones or tablets may not suit explicit necessities (data transmission, range, power consumption) of IoT-based solutions. That is the reason different IoT network protocols have been created and new ones are as yet developing. Besides, edge IoT devices and protocols are used to interact with a cloud server that processes and totals the big data arriving from different devices, performs analytics and helps in business choices [52]. IoT has turned into an indispensable piece of the present smart home, smart city, smart grid, agriculture, etc. Securing all elements engaged with an IoT system is indispensable as it includes unavoidable information gathering and dispersal.

5.2 What are the IoT applications involved in security issues?

IoT has numerous applications like an example smart home, smart city, smart health, smart grid, etc. IoT applications guarantee to bring massive incentives into our lives. With a newer wireless network, superior sensors, and progressive computing capacities, the Internet of Things (IoT) could be the following boondocks in the race for a lot of the wallet [53]. IoT applications are relied upon to equip billions of everyday devices with network connectivity and intelligence. It is as of now being conveyed widely, in different domains

[54]. Enabling devices to interface with the internet opens them up to various serious vulnerabilities on the off chance that they are not appropriately protected. Actualizing security efforts is basic to guarantee the safety of systems with IoT devices connected with them [55].

5.3 What are the challenges in IoT security devices?

This growth in popularity of IoT-connected devices prompting growth in IoT application advancement comes with a considerable amount of concerns and security challenges. We're in the time of innovation where everything has turned smart, as; mobile phones, smart home, smart city, fitness band, etc. [33]. Indeed, even a day without the internet appears to be beside outlandish today. Internet of Things (IoT) has certainly been a major aid to organizations and our lives, yet at that point, everything comes with its advantages just as the downsides which offer rise to the question in our mind, is smart truly secure? Regardless of having such a large number of exceptional and hailing benefits, IoT too faces concerns relating to security challenges [56]. There are many security challenges in IoT, the top listed security challenges have been discussed in section 4.6. Hence, on the off chance that the security challenges are dealt with, at that point IoT is certain to have a more magnificence effect in various industries [57]. In the case of the safety of information, if the threats are identified on time, the irreversible harm can be prevented. Embracing a multi-layered security approach and ensuring user information against theft, are the two greatest challenges that are required to be paid attention to very seriously as soon as possible [58]. We will at that point be familiar with a different reality where there would not be any disconnection and can generally stay awake to date.

5.4 Pros and Cons of SLR

The pros and cons of SLR conducted are identified dependent on catchphrase search. This SLR analyzed a reference rundown of chose primary studies in recognizing any extra studies. SLR likewise separates significant data consistency while lessening biases and legitimacy by creators. The cons of this SLR is that it can't guarantee that the search facilities will restore a lot of papers like a hunting procedure directed freely [59]. Along these lines, there might be different solutions given by the IoT security techniques because of the failure in catching a portion of the strategies proposed.

5.5 Suggestions for Research of SLR

This study is the first SLR led to research an investigation of security requirements for IoT applications. It is likewise the first SLR to identify security requirements related to IoT applications improvement. Our research work adds to investigate endeavors for IoT analysis particularly on security requirements for IoT applications. The security requirement analysis in this paper will guide the requirements engineer and stakeholder to examine and identify proper security requirements for any IoT applications and improve the quality of security requirements [60]. Moreover, there are likewise points of advantage for IoT engineering researchers to discover the solution, know about the process and strategy just as identify and approach related security requirements in solving challenges which have been distinguished.

6. CONCLUSION

Based on the review outcomes, the most inadequate aspect to the part of IoT security is currently authentication and authorization. The expanding number of IoT devices in our everyday lives makes authentication and security critical. To overcome security issues, security protocols are developed for the Internet of Things to decide whether they guarantee confidentiality and authenticity. The only reason why the Internet of Things needs standardized IoT protocols is to minimize the risk of security threats. Hence, this paper describes an overview of IoT security devices protocol. A systematic literature review techniques were embraced to respond to three research questions on aspects of IoT security devices protocol. The review covers the studies distributed in the range from 2010 till 2019 and ordered in ScienceDirect, Springer, IEEE, and internet sources. In a conclusion, the study demonstrates that analyzing security issues in IoT devices is rarely used in the development of IoT applications even though it is a pivotal process required from an early stage as it is highly presented to security and privacy issues. Therefore, based on the IoT application and requirements to choose one of the best security protocols which match the needs of the IoT application to keep IoT devices secure.

Acknowledgments. This project is sponsored by the Malaysian Ministry of Higher Education (MOHE) under the Fundamental Research Grant Scheme (FRGS) No. 20200102FRGS.

REFERENCES

[1] M. Alshahrani, I. Traore, and I. Woungang, "Anonymous mutual IoT interdevice authentication and key agreement scheme based on the ZigBee technique," Internet of Things, p. 100061, 2019.

[2] J. Bradley, J. Barbier, and D. Handler, "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion," Future Generation Computer Systems, 2019. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf.

[3] SAM COOK, "60+ IoT statistics and facts," April 25, 2019, 2019. [Online]. Available: https://www.comparitech.com/internet-providers/iot-statistics/.

[4] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," Futur. Gener. Comput. Syst., vol. 91, pp. 563–573, 2019.

[5] C. Riggs, J. Patel, and K. Gagneja, "Iot device discovery for incidence response," 2019 5th Int. Conf. Mob. Secur. Serv. MOBISECSERV 2019, pp. 1–8, 2019.

[6] Y. H. · Z. A. · S. H. · A. B. and A. Refoufi1, "A Review of Security in Internet of Things," Int. J. Comput. Appl., vol. 90, no. 01, pp. 20–26, 2019.

[7] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Comput. Networks, vol. 141, pp. 199–221, 2018.

[8] M. K. P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, "Lessons from Applying the Systematic Literature Review Process within The Software Engineering Domain," vol. 80, no 4, pp. 571–583, 2007.

[9] S. L. B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, "Systematic literature reviews in software engineering – A systematic literature review," – A Syst. Lit. Rev. Inf. Softw. Technol, vol. 51, no. 7, pp. 7–15, 2009.

[10] F. Ahmad and Z. Ahmad, "Blockchain in Internet-of-Things : Architecture , Applications and Research Directions," 2019 Int. Conf. Comput. Inf. Sci., pp. 1–6, 2019.

[11] K. Fan, S. Wang, Y. Ren, K. Yang, and Z. Yan, "Blockchain-based Secure Time Protection Scheme in IoT," IEEE Internet Things J., vol. PP, no. c, p. 1, 2018.

[12] and S. K. Singh, M., A. Singh, "Blockchain: A game changer for securing iot data," 2018 IEEE 4th World Forum Internet Things, pp. 51–58, 2018.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT . Challenges and opportunities," vol. 88, no. 2018, pp. 173–190, 2020.

[14] M. Tahar, B. Hammi, and P. Bellot, "Bubbles of Trust : A decentralized blockchain-based authentication system for IoT," Comput. Secur., vol. 78, no. 2018, pp. 126–142, 2020.

[15] S. Raval, "Decentralized Applications: harnessing Bitcoin's blockchain technology," First edition, O'reilly Media, 2016. .

[16] C. Gao, Z. Ling, B. Chen, X. Fu, and W. Zhao, "SecT : A Lightweight Secure Thing-Centered IoT Communication System," 2018 IEEE 15th Int. Conf. Mob. Ad Hoc Sens. Syst., pp. 46–54, 2018.

[17] "MQTT," 2019. [Online]. Available: http://mqtt.org/.

[18] S. H. Ramos, M. T. Villalba, and R. Lacuesta, "MQTT Security : A Novel Fuzzing Approach," vol. 2018, 2018.

[19] D. Dinculean and X. Cheng, "Vulnerabilities and Limitations of MQTT Protocol Used between IoT Devices," no. October 2018, 2019.

[20] R. kumar DSM, "5 reasons 'Why we choose MQTT,'" 2016. [Online]. Available: https://www.bevywise.com/blog/5-reasons-why-we-choose-mqtt/.

[21] M. Lamichhane, "Machine-to-Machine Communication : An Overview of Opportunities," Elsevier B.V., 2017.

[22] X. L. X. Li, R. Lu, X. Liang, X. Shen, J. Chen, "Smart Community: An Internet of Things Application," IEEE Commun. Mag, pp. 68–75, 2011.

[23] J. Shafiq, Z., Ji, L., Liu, A., Pang, J., & Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," IEEE/ACM Trans. Netw., no. 1, 2013.

[24] S. Jalali, "M2M Solutions – Design Challenges and Considerations," 2013 IEEE Recent Adv. Intell. Comput. Syst., pp. 210–214, 2013.

[25] D. Lars, "Performance Evaluation of M2M Protocols Over Cellular Networks in a Lab Environment," no. May 2017, 2015.

[26] J. Kim, S. C. Jaeseok, and Y. J. Lee, "Towards the oneM2M standards for building IoT ecosystem : Analysis , implementation and lessons," pp. 139–151, 2018.

[27] Y. Mehmood, C. Görg, M. Muehleisen, and A. Timm-giel, "Mobile M2M communication architectures , upcoming challenges , applications , and future directions," EURASIP J. Wirel. Commun. Netw., 2015.

[28] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," Futur. Gener. Comput. Syst., vol. 56, pp. 719–733, 2016.

[29] Q. Lyu, N. Zheng, H. Liu, J. Liu, C. A. N. Gao, and S. I. Chen, "Remotely Access '" My "' Smart Home in Private : An Anti-Tracking Authentication and Key Agreement Scheme," IEEE Access, vol. 7, pp. 41835–41851, 2019.

[30] S. T. S. Madakam, R. Ramaswamy, "Internet of Things (IoT): A literature review," J. Comput. Commun., p. 164, 2015.

[31] R. A. P. Suresh, J. V. Daniel, V. Parthasarathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," Sci. Eng. Manag. Res. (ICSEMR), 2014 Int. Conf. on, 2014, pp. 1–8, 2014.

[32] Y. Qian et al., "Towards decentralized IoT security enhancement : A blockchain approach R," Comput. Electr. Eng., vol. 72, pp. 266–273, 2018.

[33] anderson Perbits, "10 Biggest security challenges for IoT," 2019. [Online]. Available: https://www.peerbits.com/blog/biggest-iot-security-challenges.html.

[34] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," J. Syst. Archit., vol. 97, no. September 2018, pp. 185–196, 2019.

[35] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, no. 2015, pp. 17–31, 2015.

[36] R. Sairam, S. S. Bhunia, V. Thangavelu, and M. Gurusamy, "NETRA: Enhancing IoT Security Using NFV-Based Edge Traffic Analysis," IEEE Sens. J., vol. 19, no. 12, pp. 4660–4671, 2019.

[37] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," Human-centric Comput. Inf. Sci., vol. 7, no. 1, 2017.

[38] R. Hylfhv, R. Dxwkhqwlfdwlrq, G. Zlwk, K. Prgxoh, R. U. Hqfu, and S. Prgxoh, "Lightweight Iot Auth ...," pp. 1153–1155, 2017.

[39] M. A. Gurabi, O. Alfandi, A. Bochem, and D. Hogrefe, "Hardware based Two-Factor User Authentication for the Internet of Things," 2018 14th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2018, pp. 1081–1086, 2018.

[40] S. N. Ghayvat H, Mukhopadhyay S, Gui X, "WSN-and IOT-based smart homes and their extension to smart buildings. Sensors," pp. 10350–10379, 2015.

[41] H. J. Huang Z, Lin KJ, Yu SY, "Co-locating services in IoT systems to minimize the communication energy cost." 2014.

[42] T. J. Huynh SM, Parry D, Fong ACM, "Novel RFID and ontology based home localization system for misplaced objects," EEE Trans Consum Electron 60(3)402–410, 2014.

[43] A. A. Z. B. B. Zaidan, "A review on intelligent process for smart home applications based on IoT : coherent taxonomy , motivation , open challenges , and recommendations," Artif. Intell. Rev., 2018.

[44] H. H. Biswas J, Wai AAP, Tolstikov A, Kenneth LJH, Maniyeri J, Victor FSF, Lee A, Phua C, Jiaqi Z and T. T, "From context to micro-context–issues and challenges in sensorizing smart spaces for assistive living." Procedia Comput Sci 5:288–295, 2015.

[45] C. A. Sanchez I, Satta R, Fovino IN, Baldini G, Steri G, Shaw D, "Privacy leakages in smart home wireless technologies," Secur. Technol. (ICCST), 2014 Int. carnahan Conf. on. IEEE, pp 1–6, 2014.

[46] P. A. Ukil A, Bandyopadhyay S, "Privacy for IoT: involuntary privacy enablement for smart energy systems," Commun. (ICC), 2015 IEEE Int. Conf. on. IEEE, pp 536–541, 2015.

[47] Y. C. Kim YP, Yoo S, "DAoT: dynamic and energy-aware authentication for smart home appliances in internet of things," Consum. Electron. (ICCE), 2015 IEEE Int. Conf. on. IEEE, pp 196–197, 2015.

[48] M. W. Yang C, Yuan B, Tian Y, Feng Z, "A smart home architecture based on resource name service. In: Computational science and engineering," IEEE 17th Int. Conf. on. IEEE, 2014.

[49] W. S. Bhide VH, "i-learningIoT: an intelligent self learning system for home automation using IoT. In: Communications and signal processing (ICCSP)," 2015 Int. Conf. on. IEEE, pp 1763–1767, 2015.

[50] A. T. Rath, "Strengthening Access Control in case of Compromised Accounts in Smart Home," pp. 1–8, 2017.

[51] M. Hasan and A. . Fallis, "Top 15 Standard IoT Protocols That You Must Know About," 2017. [Online]. Available: https://www.ubuntupit.com/top-15-standard-iot-protocols-that-you-must-know-about/.

[52] J. M. De Fuentes, L. G. Javier, L. Pedro, and K. R. Choo, "Editorial : Security and Privacy in Internet of Things," Mob. Networks Appl., pp. 878–880, 2019.

[53] Upasana, "Real World IoT Applications in Different Domains," 2019. [Online]. Available: https://www.edureka.co/blog/iot-applications/.

[54] S. Venkatraman and B. Surendiran, "Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems," 2019.

[55] I. W. Sharon Shea, "IoT security (internet of things security)," 2018. [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security.

[56] R. Roman, J. Zhou, and J. Lopez, "On the Features and Challenges of Security & Privacy in Distributed Internet of Things," vol. 57, 2013.

[57] M. F. Elrawy and A. I. Awad, "Intrusion detection systems for IoT-based smart environments : a survey," pp. 1–20, 2018.

[58] N. Shastri, "Current Security Challenges Facing the Internet of Things," 2018. [Online]. Available: https://www.colocationamerica.com/blog/security-challenges-of-iot.

[59] M. Genero and F. P. Romero, "SLR-Tool - A Tool for Performing Systematic Literature Reviews . SLR-TOOL A Tool for Performing Systematic Literature Reviews," no. January, 2010.

[60] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain," vol. 80, no. 4, pp. 571–583, 2007.