# Review of Security Issues in Internet of Things (IoT)

Imran[1,2], Syed Mubashir Ali [1,2], Muhammad Alam[1,2], Mazliham Mohd Su'ud[2]

***Abstract*-- It is brief according to the topic that it will focus on IoT based security issues. This study will focus on rigorous literature review which will provides us trustworthy path to satisfy the industry need. In curtail IoT is not just about interconnecting embedded devices or gadgets to the Internet, however, it is also fast and continuously growing to improve the ease or satisfaction of life. The motive of IoT services is to connect the entire globe through sensors. This study reviews the IoT methodologies in the light of qualitative research. The data analysis and synthesis focus over the last three years (2018 to 2020) which are based on the PRISMA block diagram for understanding. The review identifies the IoT privacy and security issues from a different perspective and also finds out which security issue is mostly discussed in the last few years which elaborated as a basis for further research.**

**After a review of this paper, we can easily understand the different problem faces of IoT devices with the help of comparative analysis using summarize tables and graphical representation of IoT in context of the privacy and security challenges and issues face of IoT devices. After vigorous survey, it is clear that in future most of the paper will discuss data security and privacy, confidentiality, and authenticity.**

***Index Terms*—Data Security, Privacy, Confidentiality, Internet of Things**

## I. Introduction

The Internet is a robust technology that become imperative part of every human being nowadays. It has revolutionized communications, to the degree that it is presently our favored medium of daily life communication. Even in our routine life is decided after the utilization of the Internet [1], [2]. Researchers depicts after onerous circumspect assess that approximately 20-50 billion devices will connect to the internet to facilitates humans in their daily life (see figure 1).

The IoT is predictable the most significant domain of present and upcoming revolution and is increasing huge consideration from an extensive collection of several businesses [3], [4].

The Internet for Things (IoT) focuses on the Internet, It has increased its popularity in the last few years [5], [6]. IoT can be the ability to sharing data over a network without using the human-to-human or human-to-PC connection. [7], [8], [9].

The IoT can connect and respond billions of devices at a time without any delay [10], it establishes a data-sharing requirement which improves our lives rapidly [11], [12]. In other words IoT is also adopting exponential growth rate that enacts progress in every walk of life [13], [14], [15].

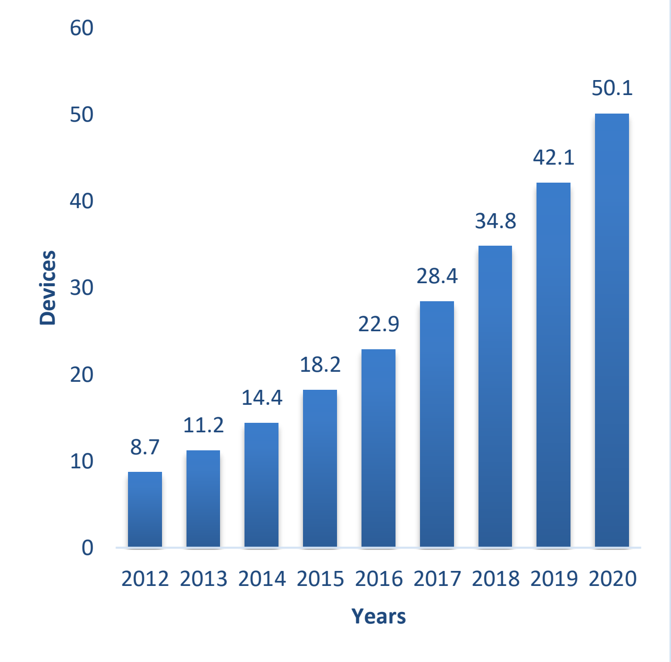

**Fig: 1. Predictable perception of smart devices by the year 2020** [16]

Therefore, in addition to conventional machines, for example, work area PC, workstations, highlight telephone versatile, and so on, all are the physical items or things that will get the capacity to speak with one another [17], [18], [19]. The IoT has

[1]Malaysian Institute of Information Technology (MIIT), Universiti Kuala Lumpur, Kuala Lumpur 50250, Malaysia
[2]College of Computer Science and Information Systems, Institute of Business Management, Karachi, Pakistan

given better opportunities in the several domain such cloud computing [20], Industrial IoT and its innovation area while carrying a few challenges to an expanded degree of concern [21], [22], [23]. Security and privacy issues in IoT situations would be considerably more challenging than what is been utilized in ordinary wireless situations [24], [25], [26].
The research is beneficial for beginners who want to learn the challenges of IoT from scratch as well as professionals [27], [28], [29]. In IoT devices the major issues are the message modification and/or alteration [30], [31], [32]. This study apprised analysis of the security and privacy for IoT. This review paper presents the categorizing the attacks under nine types of attacks from 2018 to 2020. In particular, this paper targets tending to the following exploration objectives:

1. To identify potential security issues in IoT.
2. To comprehend which IoT security issues have acquired consideration in the literature.

The paper is organized as follows. Section II provides the literature review including application domains of IoT and different security issues of IoT. Section III explores the systematic literature review protocol by using the PRISMA flowchart of included articles. In Section IV the results & discussion regarding security and privacy of IoT using the table and graphs (PI Chart). Then Section V discuss about the comparative analysis of from 2018 to 2020 era .At the end in Section VI establishes the conclusion.

## II. Literature Review

The first concept of IoT by Kevin Ashton in 1999, which has now progressed into a realism that interlinks sensors, electronic smart gadgets to the Internet [33].

### *The Security issues in IoT*

For IoT security, CIA objectives are also followed to hinder any cyber threat [34], [35]. The IoT is latest technology and has numerous limitations also which restricts its functionality in new devices or gadgets, power and its computations [36], [37], see in figure 2. The main IoT security concerns are as follows:

- **Confidentiality**

Confidentiality guarantees that delicate information are accessed to simply by an approved individual person and avoided those not approved to have them. [38] [39].

- **Integrity**

Integrity guarantees that data is in a configuration that is valid and right to its unique purposes. The recipient of the data should have the information and that can be edited by authorized persons only [40].

- **Availability**

Availability guarantees that information and resources are accessible to the individuals who need them. It is carried out utilizing strategies [16].

- **Authorization**

Authorization guarantees that the client have the necessary control authorizations or advantage to play out the activity or certain activity [40].

- **Access Control**

Access control guarantee that the security perspective mechanisms that handle and assurance access right of just approved users [41].

- **Authenticity**

Authentication is manages individual data. It incorporates approving the approaching the incoming messages against certain recognizing credentials [41].

- **Non-repudiation**

Non-repudiation is making proof to demonstrate certain activities and it guarantees that it can't be repudiated later that is accomplished by the utilization of Digital Signature and Timestamps [42].

- **Interoperability**

Interoperability means to the ability of a different systems to associate and sharing the utilization of data with each other, in one or the other access, without limitation. [43].

Confidentiality
Non-repudiation
Integrity
Security issues of IoT
Authenticity
Availability
Access Control
Authorization

**Fig: 2. Challenges of IoT Security**

## III. Systematic Literature Review Protocol

In this section shows the literature review which is focused on the eligible studies and review more than 200 papers and discuss how to filter out the numbers of papers from 2018 to 2020. The contributions of the qualitative research paper comparative of literature review papers and selected the security issues related papers of IoT devices is security. This study provides a detailed view of IoTs challenges introduced ongoing literature and which is related to the research work.
The searches by information which are related to the several privacy and security issues in the IoT from January 2018 to

December 2020. This study concentrates in the different electronic databases such as Google Scholar, Springer, IEEE, ACM, Research Gate and MDPI. This study searched 194 research papers out of which 174 papers is removed due to duplication of topic. In the screening, the titles and modified works, a sum of 111 papers were inspected in detail. However, 69 papers were related to the privacy and security based. The summarized in the PRISMA flow diagram Figure [3].

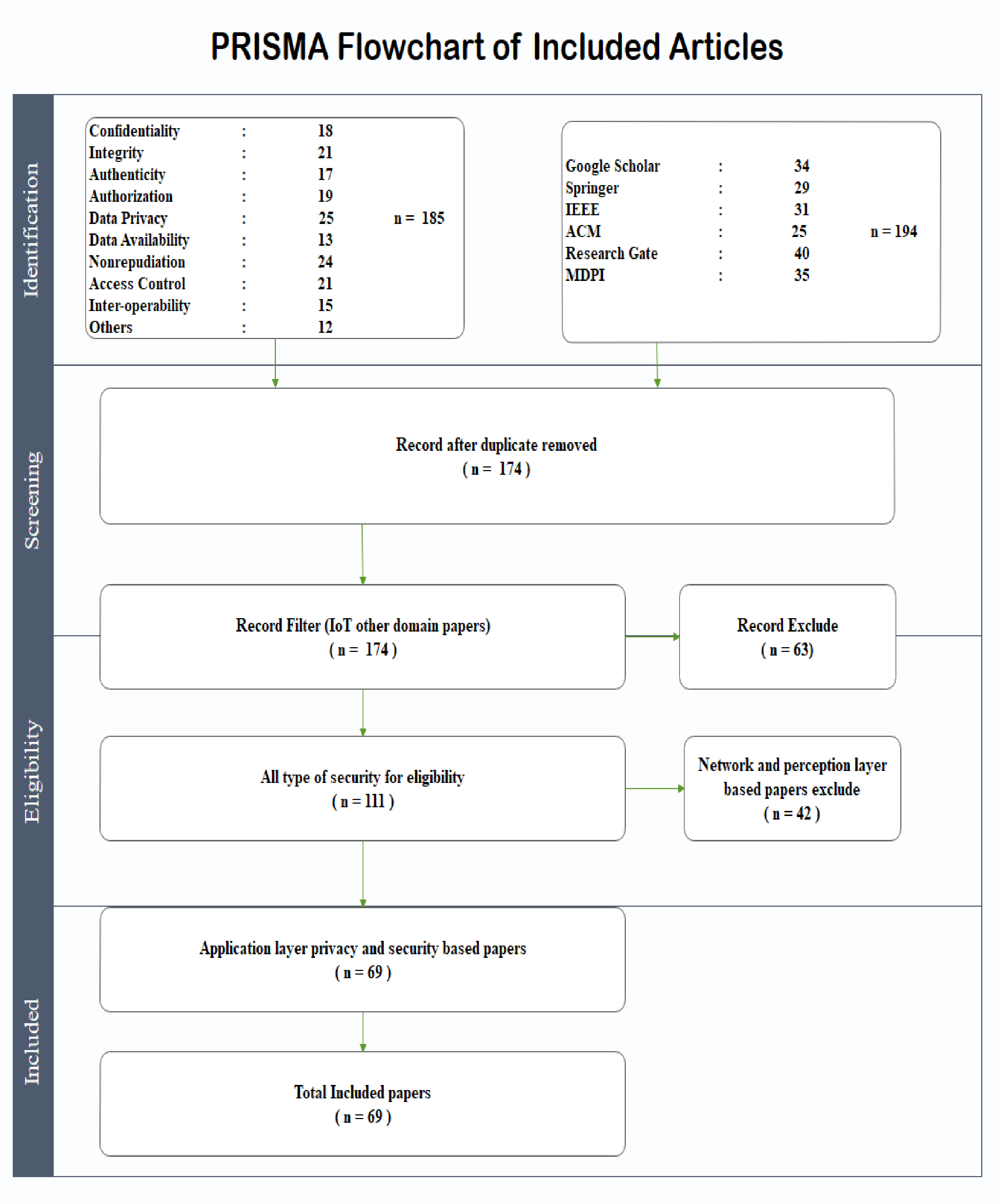

**Fig: 3. PRISMA diagram of IoT security review**

## IV. Results & Discussion

In this section, we describe the results of the literature review on IoT privacy and security which includes studies that have numerical values of data in IoT security threats using graphical representation. The tabulated format shows facts about the challenges of IoT from 2018 till 2020 the fields are reference no., year, and several issues of IoT. The graphical representation numeral each of the challenges facing IoT in a different era which is shows by using a Pie chart.

### *A. Research synthesis using the graphical and tabular form 2018 till 2020*

We distribution of paper by IoT security threats in January 2018 to December 2020, during research synthesis we found application domains of IoT security issues, numbers of papers and citations which is shown in the Tabular analysis of IoT security threats in past Table 1 and Figure 4.

**TABLE I**
**Distribution of paper by IoT security threats in future**

| Ref. No. | Year | Confidentiality | Integrity | Authenticity | Authorization | Data Security Privacy | Data Availability | Nonrepudiation | Access Control | Inter-operability |
|---|---|---|---|---|---|---|---|---|---|---|
| [44] | 2019 | | | | | √ | | | | |
| [43] | 2018 | | | | | √ | | | | √ |
| [31] | 2018 | | | | | √ | | | | |
| [30] | 2018 | | | | | | | | | |
| [45] | 2018 | √ | √ | | | √ | | | √ | √ |
| [46] | 2019 | √ | √ | | | √ | √ | | | |
| [47] | 2018 | | | | | √ | | | | |
| [11] | 2019 | | √ | √ | | √ | | | | |
| [48] | 2018 | | | | √ | | | | | |
| [24] | 2018 | | | √ | √ | √ | | | √ | |
| [39] | 2019 | √ | | | | √ | | | | |
| [38] | 2019 | | | | | | | | | |
| [49] | 2018 | | √ | | | √ | | | √ | |
| [21] | 2018 | | | | | √ | | | | |
| [50] | 2018 | | | | | √ | | | | |
| [51] | 2018 | | √ | | | | | | | |
| [52] | 2018 | | √ | √ | | | | √ | | |
| [53] | 2018 | | | | | | | | | |
| [54] | 2019 | √ | | | | | | | | |
| [55] | 2019 | | | | √ | | | | √ | |
| [40] | 2019 | √ | √ | √ | √ | √ | √ | | | |
| [56] | 2018 | √ | √ | | √ | √ | √ | | | |
| [57] | 2018 | | | √ | | | | | | |
| [58] | 2018 | | √ | √ | | √ | | | √ | |
| [59] | 2019 | | | | | √ | | | | √ |
| [60] | 2019 | √ | | | | √ | √ | | | √ |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| [41] | 2019 | | | √ | | | | | √ | |
| [61] | 2018 | | | | | √ | | | | |
| [42] | 2019 | | | | | √ | | | | |
| [62] | 2018 | | | | | √ | | | | √ |
| [63] | 2018 | | | | | √ | | | | √ |
| [64] | 2018 | | | | | √ | | | | |
| [65] | 2018 | | | | | √ | | | √ | |
| [66] | 2019 | √ | √ | √ | | √ | √ | | | |
| [67] | 2019 | | | | | | | | | √ |
| [68] | 2019 | | | √ | | √ | | | | |
| [69] | 2018 | | | | | √ | | | | √ |
| [70] | 2018 | | | | | √ | | | | |
| [71] | 2018 | √ | √ | | | √ | √ | | | |
| [72] | 2018 | √ | √ | √ | | √ | √ | | √ | |
| [73] | 2018 | √ | √ | √ | √ | √ | √ | | √ | |
| [74] | 2018 | | | √ | √ | √ | | | | |
| [74] | 2018 | √ | √ | | √ | | √ | √ | | |
| [75] | 2019 | √ | | √ | | √ | | | √ | |
| [76] | 2018 | | | | | √ | | | | √ |
| [77] | 2018 | √ | √ | √ | | | √ | | | |
| [78] | 2018 | | | | | | | | | |
| [79] | 2018 | | √ | | | √ | | | √ | |
| [80] | 2020 | √ | | | | | | | | |
| [36] | 2020 | √ | | | | | | | | |
| [81] | 2020 | | | | | √ | | | | |
| [82] | 2020 | | | √ | | | | | | |
| [83] | 2020 | √ | √ | | | | √ | | | |
| [84] | 2020 | | | | | √ | | | | |
| [85] | 2020 | | | | | √ | | | | |
| [86] | 2020 | √ | √ | √ | | √ | | | | |
| [87] | 2020 | | | | | √ | | | √ | |
| [88] | 2020 | | | | | √ | | | | |
| [89] | 2020 | | | √ | | √ | | | | |
| [90] | 2020 | | | | | | | | | √ |
| [91] | 2020 | | √ | √ | | √ | | | √ | |
| [92] | 2020 | √ | √ | √ | √ | √ | √ | | | |
| [93] | 2020 | | | | | √ | | | | |
| [94] | 2020 | | | | | √ | | | | |
| [95] | 2020 | | | | | √ | | | | √ |
| [96] | 2020 | | | | | √ | | | | |
| [97] | 2020 | | | | | √ | | | | |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total | **19** | **20** | **19** | **9** | **48** | **12** | **2** | **13** | **11** |

Fig. 4 shows the graphical representation of total number of papers from 2018 to 2020 era addressing each IoT security issue. It can be observed that “data privacy”, “confidentiality” and “integrity” with 31, 13 and 13 papers respectively and authenticity and data availability with 12 and 8 papers respectively were discussed. The most discussing security issues in the past. “Non-repudiation”, “authorization” and “inter-operability” with 1, 7 and 9 papers respectively are the least discussed IoT security issues in past era.

*Graphical Representation*

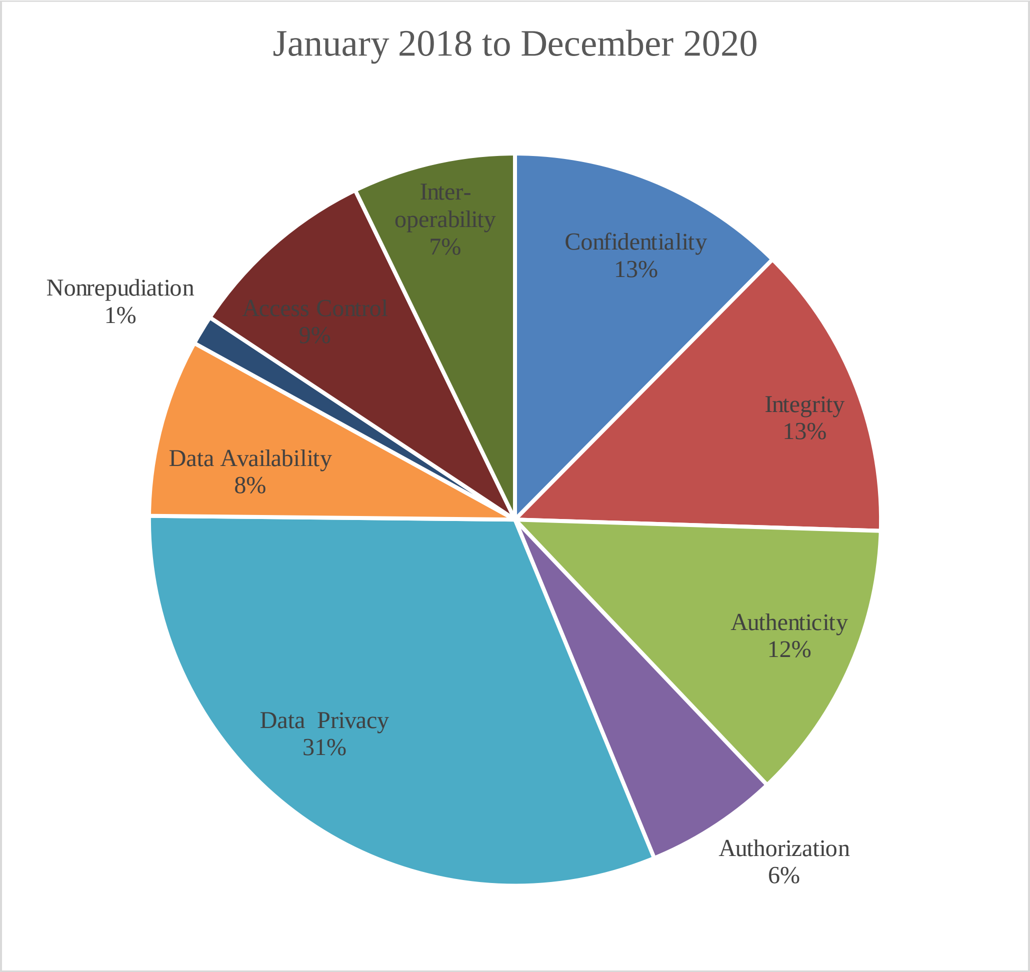

**Fig: 4. Distribution of paper by IoT security threats in future**

## V. Comparative Analysis

The comparative analysis this distribution of paper by IoT security threats in 2018, 2019 and 2020.

### *A. Confidentiality*

Figure 10 show the comparative study of IoT challenges with respect to confidentiality issue in 2018, 2019 and 2020 (see figure 5).

*Graphical Representation*

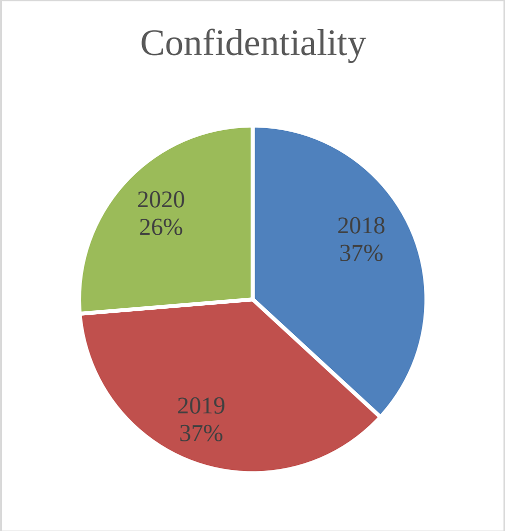

**Fig: 5. Distribution of paper with respect to confidentiality issue**

*B. Integrity*

Figure 11 show the comparative study of IoT challenges with respect to Integrity issue in 2018, 2019 and 2020 (see figure 6).

*Graphical Representation*

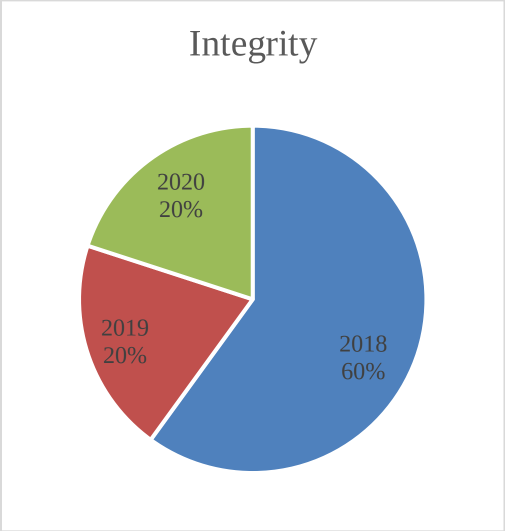

**Fig: 6. Distribution of paper with respect to integrity issue**

*C. Authenticity*

Figure 12 show the comparative study of IoT challenges with respect to Authenticity issue 2018, 2019 and 2020 (see figure 7).

*Graphical Representation*

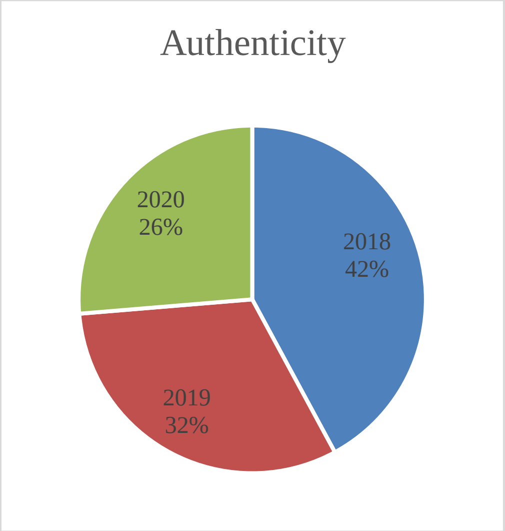

**Fig: 7. Distribution of paper with respect to authenticity issue**

*D. Authorization*

Figure 13 show the comparative study of IoT challenges with respect to Authorization issue in 2018, 2019 and 2020 (see figure 8).

*Graphical Representation*

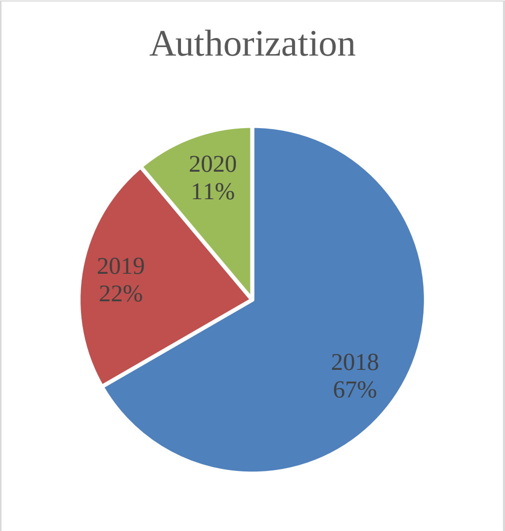

**Fig: 8. Distribution of paper with respect to authorization issue**

*E. Data Security and Privacy*

Figure 14 show the comparative study of IoT challenges with respect to data security and privacy issue in 2018, 2019 and 2020 (see figure 9).

*Graphical Representation*

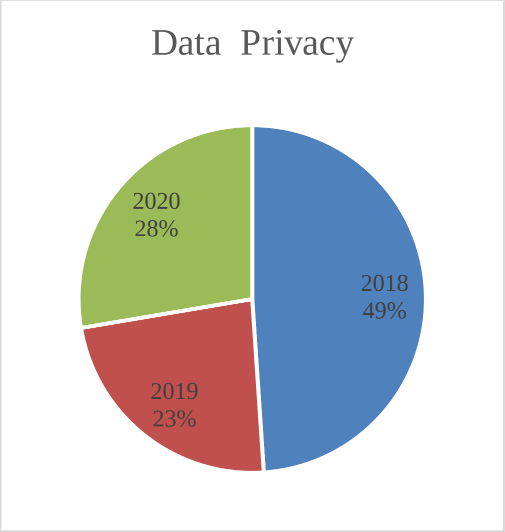

**Fig: 9. Distribution of paper with respect to data security and privacy issue**

*F. Availability*

Figure 15 show the comparative study of IoT challenges with respect to Availability issue in 2018, 2019 and 2020 (see figure 10).

*Graphical Representation*

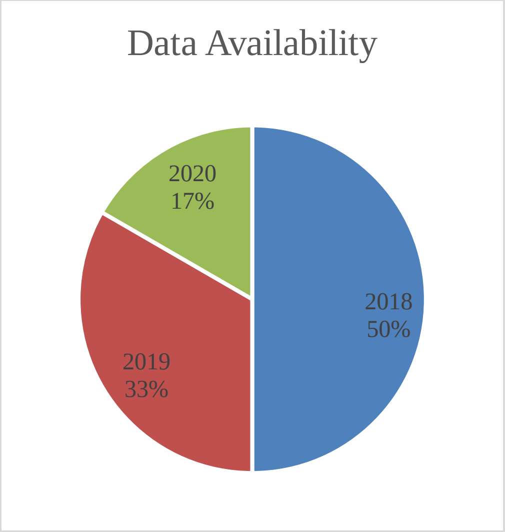

**Fig: 10. Distribution of paper with respect to availability issue**

*G. Nonrepudiation*

Figure 16 show the comparative study of IoT challenges with respect to Nonrepudiation issue in 2018, 2019 and 2020 (see figure 11).

*Graphical Representation*

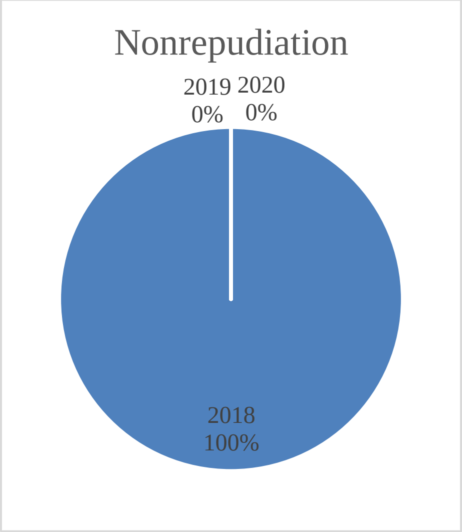

**Fig: 11. Distribution of paper with respect to nonrepudiation issue**

*H. Access Control*

Figure 17 show the comparative study of IoT challenges with respect to Access Control issue in 2018, 2019 and 2020 (see figure 12).

*Graphical Representation*

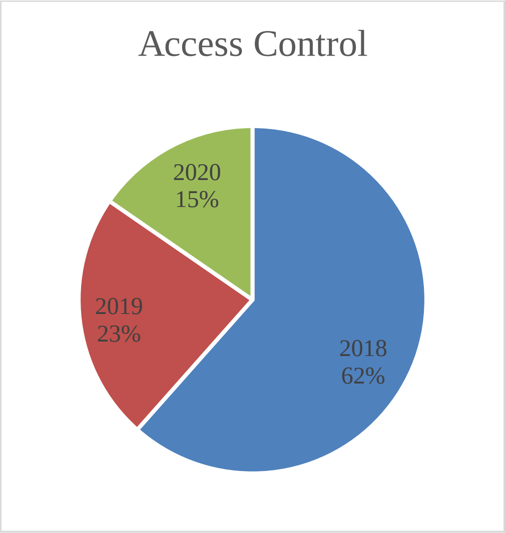

**Fig: 12. Distribution of paper with respect to access control issue**

*I. Inter-operability*

Figure 18 show the comparative study of IoT challenges with respect to data security and privacy issue in 2018, 2019 and 2020 (see figure 13).

*Graphical Representation*

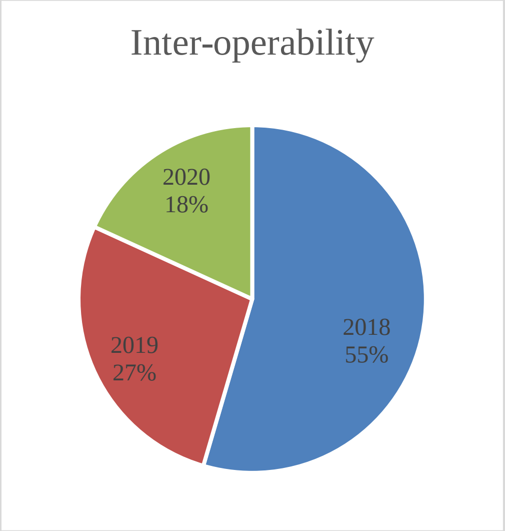

**Fig: 13. Distribution of paper with respect to inter-operability issue**

## VI. Conclusion

IoT is an emerging technology that has requirements to progress in the privacy and security area. In this paper, we have studied the comparison among the principle critical issues facing the IoT regarding security and privacy concerns. The IoT faced the several of critical issue in privacy and security. The review provided with this survey, Comparative analysis emerges different issues and focuses on research guidelines in the IoT security domain This paper has done the review of the last 3 years from 2018-2020 to focus of different security challenges in IoT and then analyzed and identified issues with respect to this era. It has been identified that "data security and privacy", "integrity" and "confidentiality are the most discussed security issues whereas "non-repudiation", "authorization" and "access control" are least discussed..

## References

[1] N. Khan *et al.*, "Big Data: Survey, Technologies, Opportunities, and Challenges," *The Scientific World Journal*, vol. 2014, pp. 1–18, 2014, doi: 10.1155/2014/712826.

[2] M. R. Belgaum, S. Soomro, Z. Alansari, and M. Alam, "Cloud Service Ranking Using Checkpoint-Based Load Balancing in Real-Time Scheduling of Cloud Computing," in *Progress in Advanced Computing and Intelligent Engineering*, vol. 563, K. Saeed, N. Chaki, B. Pati, S. Bakshi, and D. P. Mohapatra, Eds. Singapore: Springer Singapore, 2018, pp. 667–676.

[3] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on Smart Homes system using Internet-of-Things," in *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, Melmaruvathur, Chennai, India, Apr. 2015, pp. 0330–0335, Accessed: Mar. 07, 2020. [Online]. Available: http://ieeexplore.ieee.org/document/7259486/.

[4] M. R. Belgaum, S. Soomro, Z. Alansari, S. Musa, M. Alam, and M. M. Su'ud, "Challenges: Bridge between cloud and IoT," in *2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, Salmabad, Nov. 2017, pp. 1–5, doi: 10.1109/ICETAS.2017.8277844.

[5] T. Khan *et al.*, "Foreign objects debris (FOD) identification: A cost effective investigation of FOD with less false alarm rate," in *2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA)*, Putrajaya, Nov. 2017, pp. 1–4, doi: 10.1109/ICSIMA.2017.8312032.

[6] T. A. Khan, M. M. Alam, Z. Shahid, and M. M. Su'Ud, "Investigation of Flash Floods on Early Basis: A Factual Comprehensive Review," *IEEE Access*, vol. 8, pp. 19364–19380, 2020, doi: 10.1109/ACCESS.2020.2967496.

[7] Md. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," in *2015 IEEE World Congress on Services*, New York City, NY, USA, Jun. 2015, pp. 21–28, Accessed: Mar. 07, 2020. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7196499.

[8] M. A. Kamal, M. M. Alam, H. Khawar, and M. S. Mazliham, "Play and Learn Case Study on Learning Abilities Through Effective Computing in Games," in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Karachi, Pakistan, Dec. 2019, pp. 1–6, doi: 10.1109/MACS48846.2019.9024771.

[9] M. Alam, M. M. Suud, P. Boursier, S. Musa, and J. C. M. Yusuf, "Predicted and Corrected Location Estimation of Mobile Nodes Based on the Combination of Kalman Filter and the Bayesian Decision Theory," in *Mobile Wireless Middleware, Operating Systems, and Applications*, vol. 48, Y. Cai, T. Magedanz, M. Li, J. Xia, and C. Giannelli, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 313–325.

[10] S. I. Hassan, M. M. Alam, U. Illahi, M. A. Al Ghamdi, S. H. Almotiri, and M. M. Su'ud, "A Systematic Review on Monitoring and Advanced Control Strategies in Smart Agriculture," *IEEE Access*, vol. 9, pp. 32517–32548, 2021, doi: 10.1109/ACCESS.2021.3057865.

[11] M. Alamri, N. Jhanjhi, and M. Humayun, "Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review," *International Journal of Computer Science and Network Security*, vol. VOL.19 No.5, p. 15, 2019.

[12] T. A. Khan, M. Alam, Z. Shahid, and M. M. Suud, "Prior investigation for flash floods and hurricanes, concise capsulization of hydrological technologies and instrumentation: A survey," in *2017 IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS)*, Bangkok, Aug. 2017, pp. 1–6, doi: 10.1109/ICETSS.2017.8324170.

[13] A. Iftikhar, M. Alam, S. Musa, and M. M. Su'ud, "Trust Development in virtual teams to implement global software development (GSD): A structured approach to overcome communication barriers," in *2017 IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS)*, Bangkok, Aug. 2017, pp. 1–5, doi: 10.1109/ICETSS.2017.8324169.

[14] T. A. Khan, Z. Shahid, M. Alam, M. M. Su'ud, and K. Kadir, "Early Flood Risk Assessment using Machine Learning: A Comparative study of SVM, Q-SVM, K-NN and LDA," in *2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Karachi, Pakistan, Dec. 2019, pp. 1–7, doi: 10.1109/MACS48846.2019.9024796.

[15] M. W. Khan, M. A. Khan, M. Alam, and W. Ali, "Impact of Big Data over Telecom Industry," *Pakistan Journal of Engineering, Technology & Science*, vol. 6, no. 2, Feb. 2018, doi: 10.22555/pjets.v6i2.1958.

[16] M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, "A Review on Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, Mar. 2015.

[17] T. A. Khan, M. Alam, Z. Shahid, S. F. Ahmed, and Ms. Mazliham, "Artificial Intelligence based Multi-modal sensing for flash flood investigation," in *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, Bangkok, Thailand, Nov. 2018, pp. 1–6, doi: 10.1109/ICETAS.2018.8629147.

[18] A. Muhammad, P. Boursier, M. S. Mazliham, M. Shahrulniza, and J. C. M. Yusuf, "Clutter based Enhance Error Rate Table (CERT) for error correction in location estimation of mobile nodes," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, Xi'an, China, May 2011, pp. 224–228, doi: 10.1109/ICCSN.2011.6014039.

[19] M. A. Kamal, M. K. Kamal, M. Alam, and M. M. Su'ud, "Context-Aware Perspective Analysis working of RFID Anti-Collision Protocols," *jisr-c*, vol. 2, no. 16, Dec. 2018, doi: 10.31645/jisrc/(2018).16.2.02.

[20] "Highlight the Features of AWS, GCP and Microsoft Azure that Have an Impact when Choosing a Cloud Service Provider," *IJRTE*, vol. 8, no. 5, pp. 4124–4232, Jan. 2020, doi: 10.35940/ijrte.D8573.018520.

[21] S. Forsstrom, I. Butun, M. Eldefrawy, U. Jennehag, and M. Gidlund, "Challenges of Securing the Industrial Internet of Things Value Chain," in *2018 Workshop on Metrology for Industry 4.0 and IoT*, Brescia, Apr. 2018, pp. 218–223, Accessed: Dec. 26, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8428344/.

[22] M. R. Belgaum, S. Musa, M. M. Alam, and M. M. Su'ud, "A Systematic Review of Load Balancing Techniques in Software-Defined Networking," *IEEE Access*, vol. 8, pp. 98612–98636, 2020, doi: 10.1109/ACCESS.2020.2995849.

[23] "Routers Perspective Simulation-Based Analysis of EIGRP and OSPF Routing Protocol for an Organizational Model," *IJITEE*, vol. 9, no. 4, pp. 2013–2019, Feb. 2020, doi: 10.35940/ijitee.B6509.029420.

[24] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, Jan. 2018.

[25] J. Che Mustapha Yusuf, P. Boursier, M. Mohd Su'ud, and M. Alam, "Extensive overview of an ontology-based architecture for accessing multi-format information for disaster management," in *2012 International Conference on Information Retrieval & Knowledge Management*, Kuala Lumpur, Malaysia, Mar. 2012, pp. 294–299, doi: 10.1109/InfRKM.2012.6204994.

[26] M. J. Tahir, I. A. Latiff, M. Alam, and M. S. Mazliham, "Network Reconfiguration Using Modified Particle Swarm Algorithm," in *2018 2nd International Conference on Smart Sensors and Application (ICSSA)*, Kuching, Jul. 2018, pp. 1–5, doi: 10.1109/ICSSA.2018.8535944.

[27] A. Muhammad, P. Boursier, M. S. Mazliham, M. Shahrulniza, and Jawahir Che Mustapha, "Terrain/clutter based error calculation in location estimation of wireless nodes by using receive signal strength," in *2010 2nd International Conference on Computer Technology and Development*, Cairo, Egypt, Nov. 2010, pp. 95–99, doi: 10.1109/ICCTD.2010.5646073.

[28] T. Khan *et al.*, "Flash Floods Prediction using Real Time data: An Implementation of ANN-PSO with less False Alarm," in *2019 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, Auckland, New Zealand, May 2019, pp. 1–6, doi: 10.1109/I2MTC.2019.8826825.

[29] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and Its Applications: A Comprehensive Survey," *Symmetry*, vol. 12, no. 10, p. 1674, Oct. 2020, doi: 10.3390/sym12101674.

[30] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, Apr. 2018.

[31] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, Changshu, Jun. 2018, pp. 108–113, Accessed: Feb. 02, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8500488/.

[32] M. R. Belgaum, S. Soomro, Z. Alansari, M. Alam, S. Musa, and M. M. Su'ud, "Load balancing with preemptive and non-preemptive task scheduling in cloud computing," in *2017 IEEE 3rd International Conference on Engineering Technologies and Social Sciences (ICETSS)*, Bangkok, Aug. 2017, pp. 1–5, doi: 10.1109/ICETSS.2017.8324145.

[33] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, Jul. 2015, pp. 180–187, Accessed: Mar. 07, 2020. [Online]. Available: http://ieeexplore.ieee.org/document/7405513/.

[34] S. S. Basu, S. Tripathy, and A. R. Chowdhury, "Design challenges and security issues in the Internet of Things,"

in *2015 IEEE Region 10 Symposium*, Ahmedabad, May 2015, pp. 90–93, Accessed: Mar. 07, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/7166245/.

[35] M. Khan, A. Manzoor, K. Rohail, S. M. Ali, A. Iftikhar, and M. Alam, "Soft computing applications in education management — A review," in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, Bangkok, May 2018, pp. 1–4, doi: 10.1109/ICIRD.2018.8376331.

[36] C. Perera, M. Barhamgi, A. K. Bandara, M. Ajmal, B. Price, and B. Nuseibeh, "Designing privacy-aware internet of things applications," *Information Sciences*, vol. 512, pp. 238–257, Feb. 2020.

[37] A. Muhammad, M. S. Mazliham, P. Boursier, M. Shahrulniza, and J. C. M. Yusuf, "Terrain/clutter based location prediction by using multi-condition Bayesian decision theory," in *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC '12*, Kuala Lumpur, Malaysia, 2012, p. 1, doi: 10.1145/2184751.2184878.

[38] N. Miloslavskaya and A. Tolstoy, "Internet of Things: information security challenges and solutions," *Cluster Computing*, vol. 22, no. 1, pp. 103–119, Mar. 2019.

[39] S. Hameed, F. I. Khan, and B. Hameed, "Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–14, Jan. 2019.

[40] S. I. Al-Sharekh and K. H. A. Al-Shqeerat, "Security Challenges and Limitations in IoT Environments," *IJCSNS International Journal of Computer Science and Network Security*, vol. VOL.19 No.2, p. 7, 2019.

[41] I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. Vol. 14, Jan. 2019, Accessed: Mar. 20, 2020. [Online]. Available: http://arxiv.org/abs/1901.07309.

[42] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, Mar. 2019.

[43] "An Overview of Internet of Things (IoT) and Data Analytics in Agriculture: Benefits and Challenges," *IEEE INTERNET OF THINGS JOURNAL*, vol. VOL. 5, NO. 5, Oct. 2018.

[44] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, "When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities," *Journal of Industrial Information Integration*, vol. 15, pp. 21–28, Sep. 2019.

[45] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423–441, Mar. 2018.

[46] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," *Expert Systems with Applications*, vol. 133, pp. 97–108, Nov. 2019.

[47] M. Singh, A. Singh, and S. Kim, "Blockchain: A game changer for securing IoT data," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, Singapore, Feb. 2018, pp. 51–55, Accessed: Dec. 04, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8355182/.

[48] O. Alphand *et al.*, "IoTChain: A blockchain security architecture for the Internet of Things," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, Barcelona, Apr. 2018, pp. 1–6, Accessed: Dec. 15, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8377385/.

[49] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing Fog Computing for Internet of Things Applications: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 601–628, 2018.

[50] A. S. Omar and O. Basir, "Identity Management in IoT Networks Using Blockchain and Smart Contracts," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 994–1000, Accessed: Dec. 26, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8726730/.

[51] D. Fakhri and K. Mutijarsa, "Secure IoT Communication using Blockchain Technology," in *2018 International Symposium on Electronics and Smart Devices (ISESD)*, Bandung, Oct. 2018, pp. 1–6, Accessed: Dec. 26, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8605485/.

[52] S. S. Choi, J. W. Burm, W. Sung, J. W. Jang, and Y. J. Reo, "A Blockchain-based Secure IoT Control Scheme," in *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Paris, Jun. 2018, pp. 74–78, Accessed: Dec. 26, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8441717/.

[53] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018.

[54] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A Survey on Ethereum Systems Security: Vulnerabilities, Attacks and Defenses," *arXiv:1908.04507 [cs]*, Aug. 2019, Accessed: Dec. 17, 2019. [Online]. Available: http://arxiv.org/abs/1908.04507.

[55] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, Apr. 2019.

[56] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards Secure IoT Communication with Smart Contracts in a Blockchain Infrastructure," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, 2018, Accessed: Feb. 10, 2020. [Online]. Available: http://thesai.org/Publications/ViewPaper?Volume=9&Issue=10&Code=ijacsa&SerialNo=70.

[57] R. Agrawal *et al.*, "Continuous Security in IoT Using Blockchain," in *2018 IEEE International Conference on*

*Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Apr. 2018, pp. 6423–6427, Accessed: Feb. 19, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/8462513/.

[58] Y. Yu, Y. Li, J. Tian, and J. Liu, “Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things,” *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, Dec. 2018.

[59] H.-N. Dai, Z. Zheng, and Y. Zhang, “Blockchain for Internet of Things: A Survey,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019.

[60] A. Khanna and S. Kaur, “Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture,” *Computers and Electronics in Agriculture*, vol. 157, pp. 218–231, Feb. 2019.

[61] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018.

[62] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, “BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities,” *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 811–828, Apr. 2018.

[63] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, “Industrial Internet of Things: Challenges, Opportunities, and Directions,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[64] K. Sha, W. Wei, T. Andrew Yang, Z. Wang, and W. Shi, “On security challenges and open issues in Internet of Things,” *Future Generation Computer Systems*, vol. 83, pp. 326–337, Jun. 2018.

[65] J. Granjal, E. Monteiro, and J. Sa Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[66] P. I. Radoglou Grammatikis, P. G. Sarigiannidis, and I. D. Moscholios, “Securing the Internet of Things: Challenges, threats and solutions,” *Internet of Things*, vol. 5, pp. 41–70, Mar. 2019.

[67] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jun. 2019.

[68] M. binti Mohamad Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” *Computer Networks*, vol. 148, pp. 283–294, Jan. 2019.

[69] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, “Internet of Things (IoT) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018.

[70] M. Banerjee, J. Lee, and K.-K. R. Choo, “A blockchain future for internet of things security: a position paper,” *Digital Communications and Networks*, vol. 4, no. 3, pp. 149–160, Aug. 2018.

[71] D. Mendez Mena, I. Papapanagiotou, and B. Yang, “Internet of things: Survey on security,” *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 162–182, May 2018.

[72] H. F. Atlam, R. J. Walters, and G. B. Wills, “Internet of Nano Things: Security Issues and Applications,” in *Proceedings of the 2018 2nd International Conference on Cloud and Big Data Computing - ICCBDC’18*, Barcelona, Spain, 2018, pp. 71–77, Accessed: Mar. 20, 2020. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3264560.3264570.

[73] K. Chen *et al.*, “Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice,” *Journal of Hardware and Systems Security*, vol. 2, no. 2, pp. 97–110, Jun. 2018.

[74] A. K. Das, S. Zeadally, and D. He, “Taxonomy and analysis of security protocols for Internet of Things,” *Future Generation Computer Systems*, vol. 89, pp. 110–125, Dec. 2018.

[75] J. Hou, L. Qu, and W. Shi, “A survey on internet of things security from data perspectives,” *Computer Networks*, vol. 148, pp. 295–306, Jan. 2019.

[76] S. Li, L. D. Xu, and S. Zhao, “5G Internet of Things: A survey,” *Journal of Industrial Information Integration*, vol. 10, pp. 1–9, Jun. 2018.

[77] D. Mendez Mena, I. Papapanagiotou, and B. Yang, “Internet of things: Survey on security,” *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 162–182, May 2018.

[78] M. A. M. Sadeeq and S. R. M. Zeebaree, “Internet of Things Security: A Survey,” *International Conference on Advanced Science and Engineering (ICOASE)*, p. 5, 2018.

[79] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and Privacy in the Medical Internet of Things: A Review,” *Security and Communication Networks*, vol. 2018, pp. 1–9, 2018.

[80] S. Hossain, S. Waheed, Z. Rahman, S. A. Shezan, and M. Hossain, “Blockchain for the Security of Internet of Things: A Smart Home use Case using Ethereum,” *International Journal of Recent Technology and Engineering*, vol. 8, no. 5, p. 8, 2020.

[81] Y. Liu, M. Ma, X. Liu, N. N. Xiong, A. Liu, and Y. Zhu, “Design and Analysis of Probing Route to Defense Sink-Hole Attacks for Internet of Things Security,” *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 356–372, Jan. 2020.

[82] Q. Zhang and D. Xu, “Security authentication technology based on dynamic Bayesian network in Internet of Things,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 2, pp. 573–580, Feb. 2020.

[83] L. Yin, B. Fang, Y. Guo, Z. Sun, and Z. Tian, “Hierarchically defining Internet of Things security: From CIA to CACA,” *International Journal of Distributed Sensor Networks*, vol. 16, no. 1, p. 155014771989937, Jan. 2020.

[84] P. Yang, X. Kang, Q. Wu, B. Yang, and P. Zhang, “Participant Selection Strategy With Privacy Protection for Internet of Things Search,” *IEEE Access*, vol. 8, pp. 40966–40976, 2020.

[85] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of

Things (IoT) Forensics: Challenges, Approaches and Open Issues," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2020, doi: 10.1109/comst.2019.2962586.

[86] B. Mbarek, M. Ge, and T. Pitner, "An Efficient Mutual Authentication Scheme for Internet of Things," *Internet of Things*, vol. 9, p. 100160, Mar. 2020.

[87] Y. Liu, K. Xue, P. He, D. S. L. Wei, and M. Guizani, "An Efficient, Accountable, and Privacy-Preserving Access Control Scheme for Internet of Things in A Sharing Economy Environment," *IEEE Internet of Things Journal*, pp. 1–1, 2020.

[88] L. Liu, J. Su, B. Zhao, Q. Wang, J. Chen, and Y. Luo, "Towards an Efficient Privacy-Preserving Decision Tree Evaluation Service in the Internet of Things," *Symmetry*, vol. 12, no. 1, p. 103, Jan. 2020.

[89] J. Li, Z. Zhang, L. Hui, and Z. Zhou, "A Novel Message Authentication Scheme With Absolute Privacy for the Internet of Things Networks," *IEEE Access*, vol. 8, pp. 39689–39699, 2020.

[90] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers & Electrical Engineering*, vol. 81, p. 106522, Jan. 2020.

[91] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an Internet of Secure Things: A Survey on Issues and Enabling Technologies," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2020.

[92] S. Berger, O. Bürger, and M. Röglinger, "Attacks on the Industrial Internet of Things – Development of a multi-layer Taxonomy," *Computers & Security*, vol. 93, p. 101790, Jun. 2020.

[93] A. M. Basahel and M. Yamin, "Cyber Security and Privacy in Internet of Things," *International Journal of Human Potentials Management (IJHPM)*, vol. Vol.2(1), p. 11, 2020.

[94] A. A. Abd EL-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Optics & Laser Technology*, vol. 124, p. 105942, Apr. 2020.

[95] M. F. Mridha, Md. Abdul Hamid, and Md. Asaduzzaman, "Issues of Internet of Things (IoT) and an Intrusion Detection System for IoT Using Machine Learning Paradigm," in *Proceedings of International Joint Conference on Computational Intelligence*, M. S. Uddin and J. C. Bansal, Eds. Singapore: Springer Singapore, 2020, pp. 395–406.

[96] A. A. Mawgoud, M. H. N. Taha, and N. E. M. Khalifa, "Security Threats of Social Internet of Things in the Higher Education Environment," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, vol. 846, A. E. Hassanien, R. Bhatnagar, N. E. M. Khalifa, and M. H. N. Taha, Eds. Cham: Springer International Publishing, 2020, pp. 151–171.

[97] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A Survey of Internet of Things (IoT) in Education: Opportunities and Challenges," in *Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications*, vol. 846, A. E. Hassanien, R. Bhatnagar, N. E. M. Khalifa, and M. H. N. Taha, Eds. Cham: Springer International Publishing, 2020, pp. 197–209.