Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural and Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/

ISSUES, CHALLENGES, AND SOLUTION OF ARTIFICIAL INTELLIGENCE IN INTERNET OF THINGS

Syed Atir Raza[1*], Tayyaba Anees[2], Abdul Hannan Khan[3]
[1-3]Minhaj University Lahore, Pakistan
[2]University Of Management And Technology, Lahore, Pakistan

Article Info

*Corresponding Author
Email: atirrazasyed@gmail.com

Abstract

Artificial Intelligence (AI) in IoT is a unique aspect of information technology that reacts and function similarly to a humans' mind, creating automation. AI in IoT enables emulation of human intelligence to solve problems and learn to understand the high level of activities based on human-driven aspects, decision making, and the emotional cycle. However, users are yet to realize the full potential of AI in IoT systems, rendering it hard to discover and develop effective solutions to the multiple challenges encompassing this emerging technology. The challenges and issues are numerous, including difficulty in data acquisition and storage, ethics and morality issues, inadequate computation speed, flawed algorithms, weak controls and standards to help to cope up with the emerging technologies of AI in IoT, meeting human level, heavy power requirements for computing, and limited knowledge. Fortunately, some approaches can be employed to mitigate the mentioned problems and evade the adverse effects that may result from them. Examples of these approaches include establishing a long-term vision of implementation, engaging different stakeholders to support collection of huge amounts of data, controlling compliance and governance in an organization, and employing software systems to help eradicate flaws in programs.

Keywords
Artificial Intelligence, Internet Of Things, Challenges, Issues

1. Introduction

The growing urge by today's businesses to embrace AI in IoT in their operation is supported by the need to adopt automation and secure competitive advantage. However, effective operation of AI in IoT systems require that the data fed be sufficient and flawless failure to which the systems' results and predictions become compromised. However, the collaboration between Artificial Intelligence and

IoT has the potential to revolutionize the functioning of industries, businesses, and economies by availing intelligent machines, including robots in manufacturing, and retail analytics that simulates smart behavior and makes a decision with little or no human intervention. Whereas AI-enabled IoT has numerous benefits, including boosting operational efficiency, elimination of expensive unplanned downtime, and better risk management, it has several security issues and challenges. Examples include difficulty in data acquisition and storage, inadequate computation speed, flawed algorithms, weak controls and standards to help to cope with the emerging technologies in the AI-enabled IoT arena, meeting human level, heavy power requirements for computing, and limited knowledge. Nevertheless, they can be counteracted through engaging different stakeholders to support collection of huge amounts of data, controlling compliance and governance in an organization, and employing software systems to help eradicate flaws in programs.

2. Research Methodology

To unravel the challenges and issues compounding AI in IoT, more than thirty-five sources constituting journal articles and company websitesmentioned in table 1 were utilized.We have visited the websites and found them who are working in AI enabled IoT and contacted them to provide some of the information about the projects on which they are working unfortunately, they denied to provide the internal information about the projects on which they are working, which was a barrier in this research. We used the information which they have mentioned on websites andutilize that data to understand that how AI enabled IoT is working in real world and these companies are the top revenue generated companies in AI enabled IoT domain. A comparison was made among these sources to validate the challenges and issues to ensure that they were accurate and consistent. A similar comparison among the used sources was conducted to validate the solutions to the challenges and issues facing AI in IoT. In this context, challenges were regarded as obstacles that can be overcome and one can decide to set them aside and continue at any given time while they still exist. Conversely, issues were treated as difficulties that hinder achievement of specific goals.

Table 1: Companies that are working in AI enabled IoT

Company Name	Business sector
VxChange	IoT, AI, Networking
Rapid7	Information security solutions, AI enabled IoT
Sentrian	AI enabled IoT medical field.
Maana	Machine Learning , AI , IOT, BigData
Neura	Intelligently transform (AI)customer engagement by delivering behavioral attributes and real-time
Verous Systems	Uses machine learning to isolate electrical problems in motor-driven devices which are based on AI enabled IoT.
Augury Systems	Augury's machine health AI predicts machine failures in and prescribes exactly when and how to correct them.
Ring	Home security systems, Home automation.
Comfy	Robotics for commercial use, harmonize energy

2.1 Research Questions

- What are some of the challenges and issues encompassing the emerging technologies of AI in IoT?
- What are some of the approaches and solutions that can be embraced to overcome AI in IoT's challenges and issues?

3. Results

On performing a critical comparison of the different sources used, some of the most significant issues and challenges facing AI in IoT include difficulty in data acquisition and storage (Pabby & Kumar, 2017; Mohanta et al., 2020), ethics and morality issues (Stahl, 2021; Zandberg *et al.,* 2019), inadequate computation speed (Lo'ai & Saldamli, 2019; Tawalbeh *et al.,* 2020), flawed algorithms (Bertino & Islam, 2017), weak controls and standards to help to cope up with the emerging technologies (Bertino & Islam, 2017; Kolias *et al.,* 2017) of AI in IoT, difficulty in meeting human level, heavy power requirements for computing (Mellit *et al.,* 2020; Lv *et al.,* 2021), and limited knowledge on AI in IoT (McCarthy, 1987; Georgios *et al.,* 2019).

However, approaches, including establishing a long-term vision of implementation, engaging different stakeholders to support collection of huge amounts of data, controlling compliance and governance in an organization, employing software systems, and exercising transparency by organizations constitute some of the solutions to issues and challenges facing AI in IoT(Albishi *et al.,* 2017; Sahinaslan, 2019). (Soni, 2020; Alhalafi & Veeraraghavan, 2019). (Lo'ai & Saldamli, 2019). (Lo'ai & Saldamli, 2021; Harbers *et al.,* 2018).

4. Issues of Artificial Intelligence in IoT

One of the most significant issues of AI in IoT is data acquisition and storage since the systems hinge upon sensor data as their input. A substantial amount of sensor data is gathered during validation of AI in IoT systems and the presence of irrelevant and noisy data results in obstruction since they are difficult to store and evaluate. Besides, AI-enabled IoT devices operate well when a huge amount of quality and relevant data is fed making algorithms more robust (Pabby & Kumar, 2017; Mohanta *et al.,* 2020). Consequently, much need to be done on data quality and relevance since they have profound implications on outcomes and predictions to realize greater stability and precision of AI in IoT. Alongside difficulty in data acquisition and storage, ethics and morality constitute another problem of AI in IoT (Stahl, 2021; Zandberg et al., 2019). The technical training that developers are instituting in AI bots is rendering it difficult to distinguish between a machine and real customer service representative since they can flawlessly emulate human conversations (Bertino & Islam, 2017). AI in IoT'salgorithms is executed based on the assumptions of the data it is groomed on, and it can, therefore, disregard the accuracy of data (Bertino & Islam, 2017). For instance, if an algorithm is groomed on data

that mirrors racism, the resultant output will reflect it rather than automatically rectifying it. Additionally, some prevailing algorithms have mislabeled blacks as 'gorillas' which is unethical (Zewdie. & Girma, 2020). Consequently, AI-enabled IoT devices' algorithms need to be refined to make them fair, particularly when employed by private and corporate persons (Stahl, 2021). Additionally, inadequate computation speed entails another major problem of AI in IoT. AI in IoT require high levels of computational speeds availed by high-end processors (Mellit *et al.*, 2020; Lv *et al.*, 2021). However, these processors are usually expensive in terms of cost and infrastructural requirements, hindering their general embracement in AI in IoT technology. With the gradual growth of the quantity of data for processing, the computation speed requirement also heightens (Lv et al., 2021). In this regard, there is a need to develop next-gen computational infrastructure resolves to cater to the growing computational requirements as the volume of data for processing expands. Erroneous algorithms denote another malady encountered by developers in the real world and can cause legal menaces to the organization. Weak algorithms containing inappropriate sets of data can adversely affect a company's profit since they can produce incorrect and unfavorable predictions that are susceptible to legal actions (Lo'ai & Saldamli, 2019; Tawalbeh *et al.*, 2020), (Yousuf *et al.*, 2015). Furthermore, issues such as data breaches can result from poor data governance and flawed algorithm, enabling hackers to access a user's personal identification information, which typically acts as a feedstock (Saracevic *et al.*, 2020; Mahmoud *et al.*, 2015). Therefore, developing flawless algorithms is challenging to developers of AI in IoT systems, which risks an organization's profit since it is subjects to the traps of legal challenges.

New AI-enabled IoT devices are developed daily all with hidden susceptibilities primarily due to lack of adherence to standards by manufacturers. Manufacturers do not spend sufficient time and resources to address the vulnerabilities encompassing these devices, rendering it one of the primary causes of AI in IoT security issues. For example, a smart refrigerator may read Gmail login credentials, many Bluetooth fitness trackers maintain visibility after the initial pairing, and smart fingerprint locks can be hacked since they can be controlled using a Bluetooth key with a similar MAC address (Sujithra & Padmavathi, 2016; Helmi *et al.*, 2017). Absence of universal IoT security standards further deteriorates the situation since manufacturers continue developing devices with little or no security considerations in the design process of these devices. Consequently, AI-enabled IoT devices are launched with inherent security perils, including insecure data transfer and storage, inadequate update mechanisms, and hardware maladies. In this regard, non-compliance by AI-enabled IoT devices' manufacturers due to lack

of universal IoT security standards constitutes one of the considerable issues with IoT devices which can be overcome through standardization (Helmi *et al.,* 2017; Yousuf *et al.,* 2015). (Mahmoud *et al.,* 2015).

5. Challenges of Artificial Intelligence

Technologies that enable Artificial Intelligence in IoTdevices to run effectively constitute one of the major challenges surrounding these systems. The technological hurdles include poor designation and implementation of AI in IoTsystems by employing different protocols and technologies that establish multifaceted configurations, limited interfaces for AI in IoTdevices to synchronize with security devices and applications, and undefined audit and logging standards for these elements (Yousuf *et al.,* 2015; Mahmoud *et al.,* 2015). Besides, the unavailability of procedures for AI- based incident response activities and standards for substantiation and authorization constitute other technological challenges (Stahl, 2021). Consequently, advancements in technologies that enable systems of AI in IoT to operate without standardization and controls pose a major challenge (Coeckelbergh, 2020).

Alongside the lack of standardization and controls for AI in IoT systems, meeting human-level is another significant challenge. Although these systems can have an accuracy of above 90%, humans perform better (Thilakarathne, 2020) (Hussein, 2019; Vaidya & Mouftah, 2020). For instance, in a model to foretell what is contained in a given image, humans can correctly predict the output almost every time (Hussein, 2019; Vaidya & Mouftah, 2020).Contrarily, for an AI in IoTmodel to achieve a similar performance as humans, more effort would be required including, exceptional fine-tuning, hyper-parameter, huge dataset, and error-free algorithms, among others, which much work (Lo'ai & Saldamli, 2019; Tawalbeh *et al.,* 2020), (Yousuf *et al.,* 2015). Consequently, despite unceasing efforts to fine-tune AI in IoT models to realize maximum accuracy, they continue showing errors, rendering it a real struggle to reach human-level performance.

Huge amount of computing power consumed by AI in IoTdevices due to the power-hungry algorithms that they employ constitutes another challenge compounding AI in IoT (Sodhro *et al.,* 2019). The escalated power consumption is mainly due to the systems'overreliance on machine learning and deep learning which require ever-increasing cores and GPUs to operate effectively (Lv *et al.,* 2021; Liang *et al.,* 2020). Besides, numerous domains that borrows from AI's knowledge and concepts such as asteroid tracking and tracing of cosmic bodies use supercomputers that consume huge amounts of power (Liang *et al.,* 2020). Therefore, power consumption in AI remains a challenge due to incorporation of power-hungry algorithms which is a factor shunning away multiple developers (Park & Park, 2016; Cooper & James, 2009). Inadequate knowledge about Artificial Intelligence in Internet of Things remains a

challenge despite it being a better option to replace some traditional systems. As a result, numerous individuals, excluding technology aficionados, some university students, and researchers, are unaware of AI in IoT'spotential. For instance, multiple small and medium enterprises (SMEs) can schedule their work and learn innovative approaches using AI in IoTsystems to improve their performance, manage resources more effectively, and track consumer behavior to efficiently respond to market needs which they cannot due to limited knowledge (McCarthy,1987; Georgios *et al.*, 2019). Poor AI in IoTskills can also act as loopholes for malicious activities since incompetent users and workers can be tricked easily through social engineering by employing psychological manipulation to lure them into security mistakes (Sujithra & Padmavathi, 2016; Helmi *et al.*, 2017) (Gupta, 2019). Subsequently, firms need to undertake training and programs aiming to elevate skills on AI-enabled IoTsystems through strategies such as availing additional insightful workshops, newsletters, and bulletins to overcome the severe impacts the challenge might cause.

Alongside the challenges aforementioned above, customer skepticism about AI in IoT systems entail another challenge. For instance, according to a survey performed by Dutch cyber-security, 90% of IoT device users are doubtful about IoT security because they are concerned that hackers may get unauthorized access to their devices and steal important data (Newman, 2019; Andorka & Rambow-Hoeschele, 2018) (Yoon *et al.*, 2015). Consequently, IoT devices manufacturers need to contend with the skepticism of customers and address their concerns accordingly.

6. Solutions to Artificial Intelligence' Issues and Challenges

The adoption of AI in IoT continues being the driving-goal of numerous business strategies, yet data storage and acquisition is still a problem. However, having a long-term vision of execution instead of an urge for immediate and short-term gains and amassing huge pools of data can aid to overcome the problem (Lo'ai & Saldamli, 2021; Sujithra & Padmavathi, 2016). Consequently, new teams, including technologists, business strategists, and product specialists, among others need to be involved to realize change and collect a substantial amount of data (Mohanta *et al.*, 2020; Bertino & Islam, 2017). However, the teams should be monitored keenly to ensure that a consistent and harmonious approach is employed and a long-term vision is realized (Georgios *et al.*, 2019; Lo'ai & Saldamli, 2021). In this regard, AI in IoT systems can only comprehend trends and nuances by having relevant, well-defined, and quality data which can be achieved by engaging different stakeholders and working closely with large firms that have experienced rewards from AI in IoT.

Regulating compliance and governance is a potential solution to the critical challenges encompassing the intensified AI in IoT adoption

without standardization. As a result, companies should not only be required to adhere to the ever-changing compliance rules but also be allowed to leverage their data and analytics across the organization to improve awareness of their business' performance. Besides, companies should not just collect data but also be capable of evaluating it efficiently and effectively for regulatory reporting needs and strategic business planning (Alhalafi & Veeraraghavan, 2019; Mahmoud *et al.,* 2015). In this regard, companies should ensure that they are complying with regulatory requirements and be able to analyze their data efficiently and effectively.

Flawed algorithms constitute another major challenge that can, however, be overcome by developing reliable software systems. The software systems will aid in detecting errors in programs, identifying susceptibilities, and identifying best practices. Engaging security analytics is also vital, especially for less experienced developers, to aid in minimizing maladies and susceptibilities (Georgios *et al.,* 2019). Alhalafi & Veeraraghavan, 2019) Security analytics are capable of enhancing reliability in terms of AI in IoT'spredictions by assembling and scrutinizing data from diverse sources (Alhalafi & Veeraraghavan, 2019; Georgios *et al.,* 2019). Besides, they can identify malicious glitches within an AI in IoTsystem by comparing data from diverse domains. After conducting the correlation, the security analytics remedy the identified anomalies and deter them from causing harm to the connected devices (Alhalafi & Veeraraghavan, 2019). They can also detect issues in a sensor such as spikes. In this regard, engaging security analytics along with reliable software systems to detect errors is vital in overcoming security issues since they can gather valuable information to aid in the prevention of threats.

User skepticism about AI in IoT's reliance can be overcome through exercising transparency to earn customer trust. Organizations should be ready to disclose to their customers about the data collected from them, how it is utilized and stored, and measures put in place to secure it. They should also be made aware of the procedures they should take in case their devices are compromised and what alternative to take should the company experience a data breach. Consequently, organizations should consider disclosing some of the details stipulated above to dispel misconceptions they may have about AI inIoT security and instill confidence in them.

7.Conclusion

Overall, Artificial Intelligence in IoT is a technology that is capable of mimicking humans' aspects such as decision making and problem-solving to conduct specific activities independently through automation. Their adoption is coupled with numerous benefits, including boosted operational efficiency, elimination of expensive unplanned downtime, and better risk management. However, the technology is compounded by challenges that have hindered organizations from fully

embracing it in their operation. Examples of these problems include difficulty in data acquisition and storage, inadequate computation speed, flawed algorithms, heavy power requirements for computing, limited knowledge, and customer skepticism. Providentially, some measures can be upheld to overcome the mentioned problems, including engaging different stakeholders to support collection of huge amounts of data, controlling compliance and governance in an organization, employing software systems to help eradicate flaws in programs, and instilling confidence among users by exercising transparency.

8. Future Work

It may take time to realize AI in IoT vision fully but the building blocks to commence the process are ready or under development. The building blocks, including microcontrollers, microprocessors, sensors, and networking devices will work to enhance the security and confidentiality of AI in IoT devices and the universality of AI in IoT standards to render them more reliable, secure, and interoperable. Concerned stakeholders have the sole responsibility of enhancing the universality of AI in IoT standards. Besides, devising AI in IoT enabled smart machines with the capacity to simulate intelligent behavior to make accurate and informed decisions with little or no human intervention constitute another future work. Consequently, future work in AI in IoT arena will mainly aim at establishing universal standards to guide the field and improving human level in AI-enabled IoT devices to simulate intelligent behavior with more accuracy.

9. References

"Annual Report on Mana Products's Revenue, Growth, SWOT Analysis & Competitor Intelligence - IncFact." [Online]. Available: https://incfact.com/company/manaproducts-longislandcity-ny/. [Accessed: 20-Nov-2021].

"Augury Competitors, Revenue, Alternatives and Pricing." [Online]. Available: https://growjo.com/company/Augury. [Accessed: 20-Nov-2021].

"Comfy Competitors, Revenue, Alternatives and Pricing." [Online]. Available: https://growjo.com/company/Comfy. [Accessed: 20-Nov-2021].

"Neura Inc - $10.9 Million Revenue | KonaEquity.com." [Online]. Available: https://www.konaequity.com/company/neura-inc-4395481199/. [Accessed: 20-Nov-2021].

"Rapid7 Revenue 2006-2021 | RPD | MacroTrends." [Online]. Available: https://www.macrotrends.net/stocks/charts/RPD/rapid7/revenue. [Accessed: 20-Nov-2021].

"Ring Competitors, Revenue, Alternatives and Pricing." [Online]. Available: https://growjo.com/company/Ring. [Accessed: 20-Nov-2021].

"Sentrian's Competitors, Revenue, Number of Employees, Funding, Acquisitions & News - Owler Company Profile." [Online]. Available: https://www.owler.com/company/sentrian. [Accessed: 20-Nov-2021].

"Veros Systems Company Profile - Office Locations, Competitors, Revenue, Financials, Employees, Key People, Subsidiaries | Craft.co." [Online].

Available: https://craft.co/veros-systems. [Accessed: 20-Nov-2021].

"vXchnge Competitors, Revenue, Alternatives and Pricing." [Online]. Available: https://growjo.com/company/vXchnge. [Accessed: 20-Nov-2021].

Albishi, S. Soh, B. Ullah, A. & Algarni, F. (2017). "Challenges and Solutions for Applications and Technologies in the Internet of Things," Procedia Comput. Sci., 124, 608–614.

Alhalafi N. & Veeraraghavan, P. (2019). "Privacy and Security Challenges and Solutions in IOT: A review," in IOP conference series: Earth and environmental science, 322 (1), p. 12013.

Andorka S. & Rambow-Hoeschele, K. (2018). "Ethical and Social Aspects of Connected and Autonomous Vehicles: A Focus on Stakeholders' Responsibility and Customers' Willingness to Share Data," in EAI International Conference on IoT in Urban Space, pp. 17–22.

Bertino E. & Islam, N. (2017). "Botnets and internet of things security," Computer (Long. Beach. Calif)., 50 (2), 76–79.

Coeckelbergh, M. (2020). "Artificial intelligence, responsibility attribution, and a relational justification of explainability," Sci. Eng. Ethics, 26(4) 2051–2068.

Cooper J. & James, A. (2009). "Challenges for database management in the internet of things," IETE Tech. Rev., 26(5), 320–329.

Georgios, L. Kerstin, S. & Theofylaktos, A. (2019). "Internet of things in the context of industry 4.0: an overview.

Gupta, A. (2019). The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things. Apress.

Harbers, M. Bargh, M. Pool, R. Van Berkel, J. Van den Braak, S. & Choenni, S. (2018). "A conceptual framework for addressing IoT threats: challenges in meeting challenges," in Proceedings of the 51st Hawaii International Conference on System Sciences.

Helmi, O.. Sokeh, M. A & Sepidnam, G. (2017). "The challenges facing with the internet of things," Int. J. Sci. Study, 5(4), 533–537.

Hussein, A. R. H. (2019). "Internet of things (IOT): Research challenges and future applications," Int. J. Adv. Comput. Sci. Appl, 10(6), 77–82.

Kolias, C. Kambourakis, G. Stavrou, A. & Voas, J. (2017). "DDoS in the IoT: Mirai and other botnets," Computer (Long. Beach. Calif)., 50(7), 80–84.

Liang, Q. Shenoy, P. & Irwin, D. (2020). "AI on the edge: Rethinking AI-based IoT applications using specialized edge architectures," arXiv Prepr. arXiv2003.12488.

Lo'ai A. T. & Saldamli, G. (2019). "Reconsidering big data security and privacy in cloud and mobile cloud systems," J. King Saud Univ. Inf. Sci.

Lo'ai A. T. & Saldamli, G. (2021). "Reconsidering big data security and privacy in cloud and mobile cloud systems," J. King Saud Univ. Inf. Sci., 33(7), 810–819.

Lv, Z., Qiao, L. & Verma, S. (2021). "AI-enabled IoT-edge data analytics for connected living," ACM Trans. Internet Technol., 21(4), 1–20.

Mahmoud, R. Yousuf, T. Aloul, F. & Zualkernan, I. (2015). "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341.

McCarthy, J. (1987). "Generality in artificial intelligence," Commun. ACM, 30(12), 1030–1035.

Mellit, A. Hamied, A. Lughi, V. &. Pavan, A. M. (2020). "A low-cost monitoring and fault detection system for stand-alone photovoltaic systems using IoT technique," in ELECTRIMACS 2019, Springer, pp. 349–358.

Mohanta, B. K. Jena, D. Satapathy, U. & Patnaik, S. (2020). "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," Internet of Things, vol. 11, p. 100227.

Newman, D. (2019). "Return On IoT: Dealing With The IoT Skills Gap."

Pabby G. & Kumar, N. (2017). "A review on artificial intelligence, challenges involved & its applications," Int J Adv Res Comput Eng Technol, 6(10).

Park S.-H. & Park, J.-K. (2016). "IoT Industry & Security Technology Trends," Int. J. Adv. smart Converg., 5(3), 27–31.

Sahinaslan, O. (2019). "Encryption protocols on wireless IoT tools," in AIP Conference Proceedings, 2086(1), p. 30036.

Saracevic M. H. et al., (2020). "Data encryption for Internet of Things applications based on catalan objects and two combinatorial structures," IEEE Trans. Reliab.

Sodhro, A. H., Pirbhulal, S. & De Albuquerque, V. H. C. (2019). "Artificial intelligence-driven mechanism for edge computing-based industrial applications," IEEE Trans. Ind. Informatics, 15(7), 4235–4243.

Soni, V. D. (2020). "Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA," Available SSRN 3624487.

Stahl, B. C. (2021). "Ethical Issues of AI," Artif. Intell. a Better Futur., p. 35.

Sujithra M. & Padmavathi, G. (2016). "Iot security challenges and issues–an overview," Avinashilingam.

Tawalbeh, L. Muheidat, F. Tawalbeh, M. & Quwaider, M. (2020). "IoT Privacy and security: Challenges and solutions," Appl. Sci., 10(12), p. 4102.

Thilakarathne, N. N. (2020). "Security and privacy issues in iot environment," Int. J. Eng. Manag. Res., vol. 10.

Vaidya B. & Mouftah, H. T. (2020). "IoT applications and services for connected and autonomous electric vehicles," Arab. J. Sci. Eng, 45 (4), 2559–2569.

Yoon, S. Park, H. & Yoo, H. S. (2015). "Security issues on smarthome in IoT environment," in Computer science and its applications, Springer, pp. 691–696.

Yousuf, T. Mahmoud, R. Aloul, F. & Zualkernan, I. (2015). "Internet of things (IoT) security: current status, challenges and countermeasures," Int. J. Inf. Secur. Res., 5(4), 608–616.

Zandberg, K. Schleiser, K. Acosta, F. Tschofenig, H. & Baccelli, E. (2019). "Secure firmware updates for constrained iot devices using open standards: A reality check," IEEE Access, vol. 7, pp. 71907–71920.

Zewdie T. G. & Girma, A. (2020). "Iot Security And The Role Of Ai/Ml To Combat Emerging Cyber Threats In Cloud Computing Environment.," Issues Inf. Syst., 21(4).