Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 125-133, 5, 2023

Araştırma Makalesi

IJANSER
https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 125-133, 5, 2023

Research Article

Security and Fire Safety of Industries with AI and IoT Devices

Abdullah Ashraf*

[1]*Department of Electrical Engineering, University of Engineering and Technology Taxila, Pakistan*

(abdullah.ashraf@students.uettaxila.edu.pk) Email of the corresponding author

(Received: 05 June 2023, Accepted: 20 June 2023)

(1st International Conference on Pioneer and Innovative Studies ICPIS 2023, June 5-7, 2023)

ATIF/REFERENCE: Ashraf, A. (2023). Security and Fire Safety of Industries with AI and IoT Devices. *International Journal of Advanced Natural Sciences and Engineering Researches, 7(5), 125-133.*

Abstract – Ever-increasing advancement in the field of Artificial Intelligence (AI) has caused a spike in the implementation of the Internet of Things (IoT) devices in the industrial as well as the commercial environment. This also demands its assimilation in the sector of power systems, mainly the security and safety part of the power system which faces the most negligence. This paper underlines the economic losses caused by the laxness shown in this department of power and proposes the practices to minimize such losses using AI integrated into IoT devices in the grid and other areas of the power sector. The research focuses on the safety of humans from fires or intruders as well as from any part of the grid which can be a fire hazard if neglected.

Keywords – Safety, Security, Internet of Things, Arduino, NodeMCU

I. INTRODUCTION

Mishaps caused by fire are the most common type in any industrial sector and as studied in [1] even with the decline in deaths by fire observed throughout the globe [2], if eviction time exceeds the time limit of 20 minutes, the damage caused to the people will increase significantly [3]. A study by Machtar et. al [4] showed that periodically monitoring the Fire Safety Management (FSM) program can lead to reduced losses through fires as most of the organizations neglect FSM which ultimately causes losses of human lives and machinery. A similar study to research the sociological factors of fire safety was done in [5]. Most of the buildings will desegregate safety measures in case of fire and are likely to build fire emergency exits in an event of fire accident. But, the likelihood of those passages being blocked by the fire itself is not implausible and will even cause more damage to the people trying to evacuate from that very exit. The study in [6] showed the methodology to implement the expert system using Bayesian Belief Network (BBN) which proved to be a great fire analysis solution. In [7] a great method is suggested which uses IoT protocols in providing the safest and fastest desertion path in real-time for the evacuation. The number of internet-connected devices is now more than the number of people on Earth [8] and is predicted to reach 500 billion by the year 2030 [9]. The study in [10] reveals an AI-based system that integrates itself into the environment same as Amazon's Alexa or Microsoft's Cortana. Using both strategies we can create a system capable of providing the best path in case of fire in any type and size of the industry. Power sector industries are mostly huge, thus the use of CCTVs and an IoT system discussed in the above studies can help a lot with advancing the safety precautions. In [11] a system for trespasser detection is implemented with CCTVs and an alarm system using the same

computer vision methodology as the study in [12]. The method of comparing the frames of the footage with the static frame indicates the presence of an intruder. In [13] a system is suggested which describes the intrusion detection system using network as base of communication, it alarms the authorities in case of any invader possibility. The study also proposes a Machine Learning (ML) approach in building the Intrusion Detection and Prevention System (IDPS) which is considered here as well. This paper projects the best methods up-till-date to minimize the devastation caused by fire disasters and prevent the losses due to unauthorized human intervention in the power system industry.

II. Components of IoT

The term "internet of things" has seen a spike in interest in this decade, but the term was more than two decades old as was first used by Ashton in 1999 [14] and was defined as a development of the internet with all the objects of daily use connected to it [15], and with the rise of wearables and automation systems it is certainly becoming a thing of great interest. Figure 1 shows a general diagram of an IoT system.

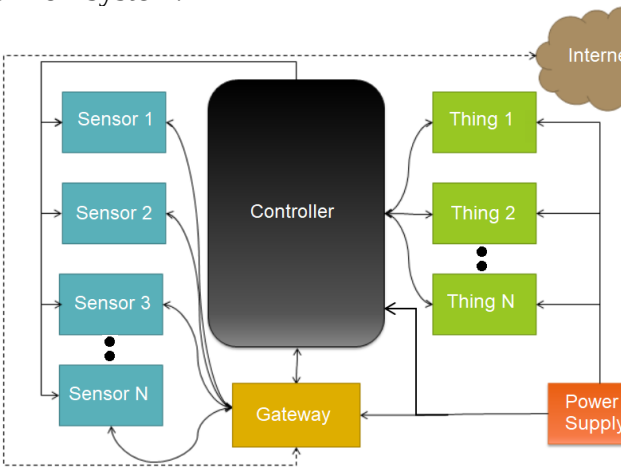

Fig. 1: IoT system components

A. *Internet*

The main segment of the system. This needs to be assessable all the time for the IoT system to be successful. The reliability of this component can be affected by natural disasters like hurricanes, tornados, earthquakes, etc. [16].

B. *Gateway*

This part of the system acts as a bridge between the cloud part and the real-world part of the system. In the complete system, this part is the most vulnerable to security attacks. The first effort to make this system secure was done by Bill in 1990 [17]. But the problem is far from being solved, as with every problem solved, a new vulnerability arises every time an old one is solved. Mostly the gateway is wirelessly connected to the internet and is wired with the sensors and things part of the system. For a wireless system, some characteristics are a must-have in the industrial environment.

a) High range: At least 50m in "cluttered" industrial RF environments where there is often a lot of metal in equipment and building structure and increasing amounts of radio interference [18].

b) High data rate: In industrial sensing and control applications required data rates vary widely by application but are often low and/or intermittent.

c) Low network latency: This varies widely by the application. It should ideally be possible to tune the network availability or response to the application requirement at the end-node to optimize performance. A second consideration is how long new devices take to join the network.

d) Reliable power profile: Ideally under all circumstances, devices would be battery-operated to avoid both power and data wiring costs and increase flexibility.

e) Security status: At the lowest level, how sure can one be that the data did get from origin to endpoint accurately and completely? This is critical in sensing and control applications where humans do not normally validate data at the operating time interval [19]. At the highest level, how sure can one be that my network and its data cannot be "hacked" and the data misappropriated or meddled with? Is the person able to control which devices join my network?

C. *Sensors*

This is the reading part of the system which takes on real-world data and pass it on to the controller for processing purpose. Over the years many different types of sensors were produced, some of which include electrochemical [20], capacitive [21], fibre grating [22], micro inertial [23], etc.

D. Internet

This is the brains of the system which will obtain the data from the sensor, make decisions based on that data, and then if the result is to be sent to a thing, it will do so as well. The most used controllers in IoT are studied by Steane and Radcliffe [24]. Some of the more widely known controllers in the automation part of IoT are Arduino, Raspberry Pi, and ATMEL.

E. Things

This can be any electronic device capable of understanding the single sent by the controller and act upon it accordingly.

III. Fire Safety

The safety of humans in case of fire by creating evacuation paths in the building was first introduced in the 20th Century [25] with the start of this study many methods to evacuate people in case of a fire outbreak were presented. At the end of the century, the focus was shifted towards the human part of fire safety, the people. Their behaviors were studied [26] and based on those behaviors. The study to evacuate people with disabilities was started in the 1970s [25] with the results of the research implemented in the 1980s.

Survival of humans in case of a fire outbreak was based on some factors as mentioned in the book [27]:

i. Awareness of the outbreak
ii. Responding to the indicators of the outbreak
iii. Moving to a safe place with being in the least possible panic state.

The lack of awareness, in many cases, can be fatal in the case of such outbreaks.

A. Fire detection

Fire detection can be done by many sensors readily available nowadays. Most of these sensors are infrared based while some smoke sensors are also used in place of fire sensors.

Fire detection methods in open areas, such as forests and fields were discussed in [28] and [29] which proposed the use of satellites to detect fires. In the case of mostly closed areas like those of industries, research like [30] proposed the use of surveillance videos along with neural networks to detect fires. Six algorithms for detecting fires were also introduced by Giglio et. al in [31].

B. Fire Prevention

Techniques to prevent fires in buildings were studied. In a developed country with skyscrapers and high population density, fires are best prevented before it occurs as done in [32] for the country of Taiwan. Mostly caused household fires can be prevented by installing a gas leakage detection system in the home environments as proposed in [33] where ZigBee was used as a means of communication between sensors and the main network. The method also introduced a way to reduce false alarms in case of fire to almost zero percent, by using three different types of sensors (temperature, smoke, and gas sensors) to validate that there is a case of fire while being energy efficient as well. A study by Vimal and Nigam [34] introduced a method to prevent fires using WSN along with IoT. The problem with this system was its requirements of a lot of network nodes in the wild for detection.

IV. Artificial Intelligence

Artificial intelligence is not just the idea of making computers clever fakes of humans, but to make them surpass the intelligence of humans [35]. The idea is not new, it has been discussed since the invention of computers themselves. The concept was not of any use at the time of its creation, but with internet and large data repositories now available, it does not seem as foreign as it was in the 1960s. In recent years, AI has seen many advancements and has piqued the interest of software giants like Google and Microsoft, but the rise of this field has also created trust-issues among communities that view it as evil [36]. Some of the ethical issues in this field were discussed [37]. AI and Machine learning are often used in the same sense as their boundaries are a blur to this day. Machine learning methods have been used in the field of cybersecurity [38] and can be applied to IoT systems as well.

The automation of daily life tasks has been researched since long ago [39].

V. Method of Analysis

Many methods to prevent fires were studied over the years and some of which are mentioned below. These methods were researched and implemented in many industrial fields with experimental data also obtained.

A. Thermal Imaging

Using computer vision paired with thermal imaging cameras the study in [12] proposes a method to safely prevent any mishaps causing fire hazards in the vicinity. The study represents a way for a MATLAB based GUI program to warn the workers in the facility of a possible fire hazard when a person gets in the way of potentially heat emitting bodies, which in the case of power system industry can be most of the transformer side equipment. Computer vision has a different view of images than our own. The levels of image representation are shown in Figure 2.

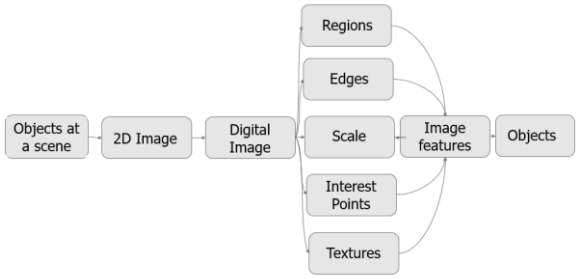

Fig. 2: Levels of image representation[40]

The method, in this case, works by using the thermal images captured by the thermal camera and then creating a warning signal waking up the safety measures in the facility in case a person is in a dangerous area.

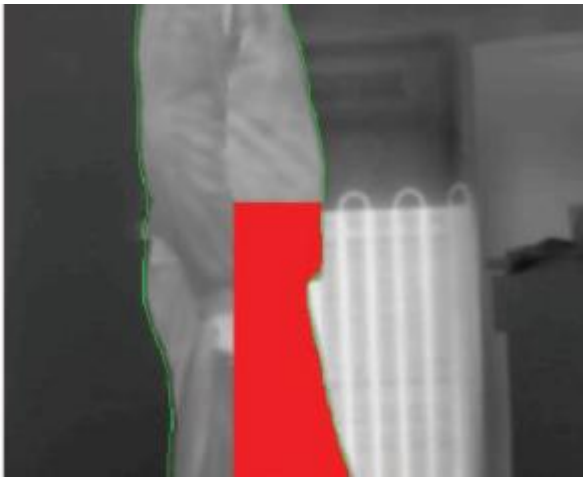

Fig. 3: Detection of a human in the danger zone[12]

A similar study in [41] is also using image processing in the firecrackers industry where fire emergencies are no surprise. The study in [42] proposes a method of communication in such industry using IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) and Routing Protocol for Low power and Lossy Networks (RPL) based Industrial Wireless Sensor Networks (IWSN) as they offer low latency in such areas.

B. AI Approach

An intelligent software system was developed in [43] but was not as sophisticated as the systems which can be developed by the current technologies. An artificially intelligent system was also patented in [44]. A neural-fuzzy interference system was proposed in [45] with the structure as shown in Figure 4. The system was designed to prevent forest fires and to uses a hybrid AI approach which was termed as Particle Swarm Optimized Neural-Fuzzy (PSO-NF). The study initially selected 10 fire ignition factors and based the study on them. The factors were selected by viewing the past forest fires. This study showed great results from simulations.

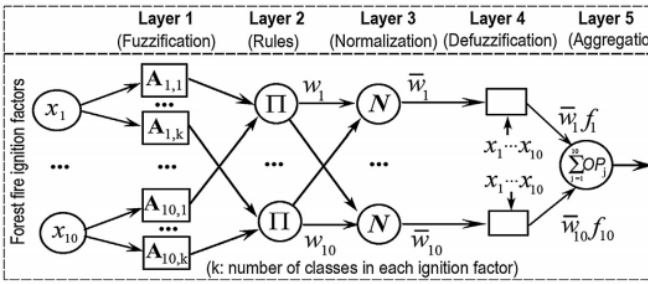

Fig. 4: Neural Fuzzy interference system

C. Smart IoT and Soft AI

The method proposed in [10] can be implemented in the power industry as well as many others like

those. The system here is comprised of small GENOMEs (Geolocated Natural language Objects for Memory Evocation) shown in Figure 5 which are placed at the sidewalks and can analyze speech data and can guide the evacuees in case of any fire emergency by using and detecting potentially useful phrases like "This path is closed due to fire" or "move to the north side of the building" etc. The shapes of IoT devices were like small creatures. The chatbot system used in the system was developed by Google's "dialog flow system" [46]. This system can provide data to the safety department about the location where the evacuees will come from and save many lives in such conditions.

Fig. 5: Gnomes used in Olympic parks

D. *Building structure modifications*

Studies in [47-49] modify the designs of buildings mostly susceptible to fires. FIERAsystem developed in [47] analyzes buildings for fire safety and risk management. The steel portal design in [49] assured that in case of any fire the building won't fall on the personals present in the building, and will fall outward in case of damage. A study in [48] showed a decision analysis of a building concerning the damage to human life. The study provided a risk assessment for evacuees in a fire disaster.

E. *Fire detection and evacuation*

Many fire safety guidebooks were produced over the years which are helpful in the prevention of fires and evacuation strategies in case of fire [50][51]. The study in [52] shines a light on a technique to reach the people in case of a fire disaster in a fast and efficient way. As most of the people in industries carry their smartphones or company Personal Digital Assistants (PDAs) to their worksite, they can be located using the wireless access points or APs and can be communicated individually to guide them to the path to safety without putting their lives in danger. The Wireless Sensor Networks (WSN) can share information with the centralized server which can calculate the shortest and safest path and then can communicate to the people in danger via PDAs or the system proposed in [10].

As most of the people carry smartphones with them everywhere, a system using this part of the society nowadays was presented [32] which uses Building Information Modeling. Unlike the previous method, this method uses building's model which must be fed in the application beforehand and also the GPS on the devices to take the humans inside the danger zone to the safe zone and it also guides them towards the rescuers using the same built-in GPS sensor of modern mobile devices. This system works by detecting the fires through internet-connected fire sensors and then guide the evacuees to the nearest safe area. The mobile application developed for this purpose was able to help both evacuees and firefighters in this case of an emergency.

Research in [53] and [54] also used IoT to prevent fires. Study in [53] used AI to detect the fires and was successful in fire prevention as it also communicates the alerts to the authorities in case of any fire outbreak is detected. The system used neural networks with the Kaggle forest fire dataset as training data and was able to achieve 96.7% accuracy.

The Tensor board model used in this study is shown in Figure 6.

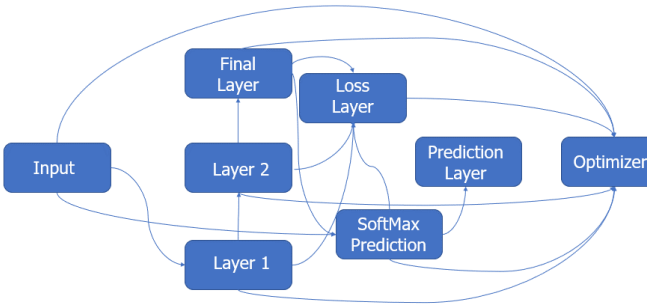

Fig. 6: Tensor visualization model

VI. Security and Reliability of IoT

A. *Security of WSN based IoT devices*

The security of IoT devices is the main cause of concern. The security risks of this system cannot be eliminated but can be minimized using proper protocols and having proper safety measures in place. In [55], a method to have reliable IoT applications in the industrial sector is proposed which applies multi-layer safety and security protocols. In [56], all the concerns regarding IoT are studied and the safety concerns for each sector are shown.

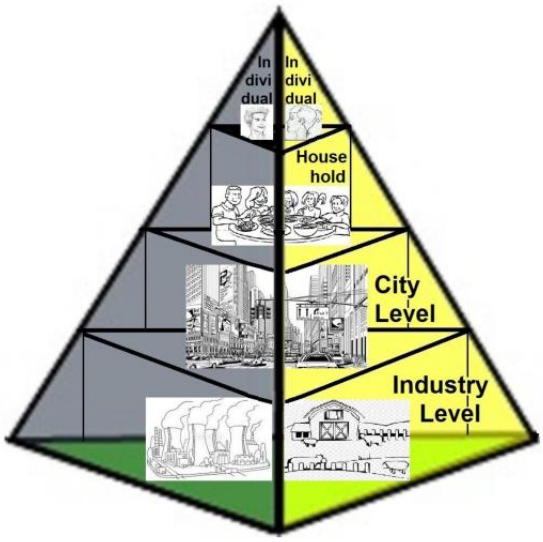

Figure 7: IoT safety concerns using a layered perspective[56]

B. *Reliability*

In [57] the reliability of IoT devices is studied and a solution to not use iterative type Temporal Topology Control Protocols (TTCPs) was suggested as it can hinder the reliability of the system. The solution also works for the systems where battery life is of concern and the system works on battery life instead of the direct power line connection. Comparison of Message Queue Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) in [58] concluded that using MQTT was the best option as it has substantial reliability and low power requirements compared to CoAP. MQTT was also found to outperform CoAP in terms of latency by 80%.

VII. Results

The way to reduce fire losses in the case of the power sector is to use the method proposed in [12] with its integration to IoT devices with AI can lead to a great fall in the damages caused by such disasters similar to the case in [45]. The protocol for communication between the IoT devices should be MQTT as it was shown to be superior to CoAP in this regard.

VIII. Conclusion

This study reviews most of the methods used for fire prevention and safety in the industrial sector. It showcased a different methodology to detect and prevent fires using AI and IoT. The review discusses different methodologies observed in past researches and contributes a new and improved way of fire prevention method using an integrated system of the past research.

References

[1] A. Mahgoub, N. Tarrad, and R. Elsherif, “IoT-Based Fire Alarm System,” pp. 162–166, 2019.

[2] U.S. Fire Administration, “Fire Death Rate Trends : An International Perspective,” Top. Fire Rep. Ser., vol. 12, no. 8, pp. 1–8, 2011.

[3] C. S. Ryu, “IoT-based intelligent for fire emergency response systems,” Int. J. Smart Home, vol. 9, no. 3, pp. 161–168, 2015, doi: 10.14257/ijsh.2015.9.3.15.

[4] H. K. Muchtar, H. Ibrahim, and S. Raodhah, “Analisis Efisiensi dan Efektivitas Penerapan Fire Safety Managemen dalam Upaya Pencegahan Kebakaran di PT. Consolidaeted elektrik Power Asia Kabupaten Wajo.,” Higene, vol. 2, no. 2, pp. 92–98, 2016.

[5] G. Spinardi, L. Bisby, and J. Torero, “A Review of Sociological Issues in Fire Safety Regulation,” Fire Technol., vol. 53, no. 3, pp. 1011–1037, 2017, doi: 10.1007/s10694-016-0615-1.

[6] E. Chojnacki, W. Plumecocq, and L. Audouin, “An expert system based on a Bayesian network for fire safety analysis in nuclear area,” Fire Saf. J., vol. 105, no. January, pp. 28–40, 2019, doi: 10.1016/j.firesaf.2019.02.007.

[7] H. Muccini, C. Arbib, P. Davidsson, and M. Tourchi Moghaddam, “An IoT Software Architecture for an Evacuable Building Architecture,” Proc. 52nd Hawaii Int. Conf. Syst. Sci., vol. 6, pp. 678–687, 2019, doi: 10.24251/hicss.2019.083.

[8] I. Analytics, “State of the IoT 2018: Number of IoT devices now at 7B--Market accelerating,” IoT Anal. Available https//iot-analytics. com/state-ofthe-iot-update-q1-q2-2018-number-of-iotdevices-now-7b/.[Accessed 27-Mar-2019], 2018.

[9] C. Tran and S. Misra, “Review: The Technical Foundations of IoT,” IEEE Wirel. Commun., vol. 26, no. 3, pp. 8–8, 2019, doi: 10.1109/mwc.2019.8752474.

[10] R. Milton, D. Hay, S. Gray, B. Buyuklieva, and A. Hudson-Smith, “Smart IoT and soft AI,” IET Conf. Publ., vol. 2018, no. CP740, pp. 1–6, 2018, doi: 10.1049/cp.2018.0016.

[11] P. Ghadi, S. Surve, A. Tiwari, R. Vaykole, and P. D. V Thombre, “Intruder Detection System using Camera with Alert Management,” pp. 1339–1341, 2019.

[12] M. Zubal’, T. Lojka, and I. Zolotová, “IoT gateway and industrial safety with computer vision,” SAMI 2016 - IEEE 14th Int. Symp. Appl. Mach. Intell. Informatics - Proc., pp. 183–186, 2016, doi: 10.1109/SAMI.2016.7423004.

[13] M. S. Husain, “Nature Inspired Approach for Intrusion Detection Systems,” Des. Anal. Secur. Protoc. Commun., pp. 171–182, 2020, doi: 10.1002/9781119555759.ch8.

[14] A. Kevin, “That ’ Internet of Things ’ Thing,” RFiD J., p. 4986, 2010, doi: 10.1038/nature03475.

[15] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, “A survey based on Smart Homes system using Internet-of-Things,” 4th IEEE Spons. Int. Conf. Comput. Power, Energy, Inf. Commun. ICCPEIC 2015, pp. 330–335, 2015, doi: 10.1109/ICCPEIC.2015.7259486.

[16] L. Quan, J. Heidemann, and Y. Pradkin, “Trinocular: Understanding internet reliability through adaptive probing,” Comput. Commun. Rev., vol. 43, no. 4, pp. 255–266, 2013, doi: 10.1145/2534169.2486017.

[17] B. Cheswick, “The Design of a Secure Internet Gateway,” Proc. Summer USENIX Conf., pp. 233–237, 1990.

[18] P. Dhillon and P. Malhotra, “A Review paper on History , Current trends and Future of Zigbee (IEEE 802 . 15 . 4) Standard,” 2013.

[19] M. S. Nair, R. Jishnu, K. M. Rakesh, and A. Ramachandran, “Implementation of a web-based programming tool for distributed, connected Arduino systems,” 2016 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2016, pp. 1595–1600, 2016, doi: 10.1109/ICACCI.2016.7732276.

[20] C. C. Liu, “Electrochemical sensors,” Med. Devices Syst., vol. 74, no. 12, pp. 48-1-48–6, 2006, doi: 10.5796/kogyobutsurikagaku.58.1087.

[21] L. K. Baxter, “Capacitive sensors,” Des. Appl., 1997.

[22] S. Zhang, S. Bae Lee, X. Fang, and S. Sam Choi, “In-fiber grating sensors,” Opt. Lasers Eng., vol. 32, no. 5, pp. 405–418, 1999, doi: 10.1016/S0143-8166(99)00052-4.

[23] C. Song, B. Ha, and S. Lee, “Micromachined inertial sensors,” IEEE Int. Conf. Intell. Robot. Syst., vol. 2, no. 8, pp. 1049–1056, 1999, doi: 10.1109/iros.1999.812819.

[24] T. Steane and P. J. Radcliffe, “Multiple Intermittent Controllers for IoT Home Automation,” 2018 28th Int. Telecommun. Networks Appl. Conf. ITNAC 2018, pp. 1–6, 2019, doi: 10.1109/ATNAC.2018.8615433.

[25] M. Kobes, I. Helsloot, B. de Vries, and J. G. Post, “Building safety and human behaviour in fire: A literature review,” Fire Saf. J., vol. 45, no. 1, pp. 1–11, 2010, doi: 10.1016/j.firesaf.2009.08.005.

[26] “Integrating Human Behavior Factors into Design,” SFPE Guid. to Hum. Behav. Fire, no. 28, pp. 3–11, 2019, doi: 10.1007/978-3-319-94697-9_2.

[27] H. Frantzich and L. universitet. Institutionen för brandteknik, A Model for Performance-based Design of Escape Routes. Department of Fire Engineering, Lund Institute of Technology, Lund University, 1994.

[28] W. Schroeder, P. Oliva, L. Giglio, B. Quayle, E. Lorenz, and F. Morelli, “Active fire detection using Landsat-8/OLI data,” Remote Sens. Environ., vol. 185, pp. 210–220, 2016, doi: 10.1016/j.rse.2015.08.032.

[29] C. Yuan, Z. Liu, and Y. Zhang, “Fire detection using infrared images for UAV-based forest fire surveillance,” 2017 Int. Conf. Unmanned Aircr. Syst. ICUAS 2017, pp. 567–572, 2017, doi: 10.1109/ICUAS.2017.7991306.

[30] K. Muhammad, J. Ahmad, I. Mehmood, S. Rho, and S. W. Baik, “Convolutional Neural Networks Based Fire Detection in Surveillance Videos,” IEEE Access, vol. 6, no. c, pp. 18174–18183, 2018, doi: 10.1109/ACCESS.2018.2812835.

[31] L. Giglio, W. Schroeder, and C. O. Justice, “The collection 6 MODIS active fire detection algorithm and fire products,” Remote Sens. Environ., vol. 178, pp. 31–41, 2016, doi: 10.1016/j.rse.2016.02.054.

[32] M. Y. Cheng, K. C. Chiu, Y. M. Hsieh, I. T. Yang, J. S. Chou, and Y. W. Wu, “BIM integrated smart monitoring technique for building fire prevention and disaster relief,” Autom. Constr., vol. 84, no. August, pp. 14–30, 2017, doi: 10.1016/j.autcon.2017.08.027.

[33] F. Saeed, A. Paul, A. Rehman, W. H. Hong, and H. Seo, "IoT-Based intelligent modeling of smart home environment for fire prevention and safety," J. Sens. Actuator Networks, vol. 7, no. 1, 2018, doi: 10.3390/jsan7010011.

[34] V. Vimal and M. Ji Nigam, "Forest Fire Prevention Using WSN Assisted IOT," Int. J. Eng. Technol., vol. 7, no. 3.12, p. 1317, 2018, doi: 10.14419/ijet.v7i3.12.17877.

[35] J. Haugeland, Artificial intelligence: The very idea. MIT press, 1989.

[36] F. K. Dosilovic, M. Brcic, and N. Hlupic, "Explainable artificial intelligence: A survey," 2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc., pp. 210–215, 2018, doi: 10.23919/MIPRO.2018.8400040.

[37] D. Greene, A. L. Hoffmann, and L. Stark, "Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning," Proc. 52nd Hawaii Int. Conf. Syst. Sci., pp. 2122–2131, 2019, doi: 10.24251/hicss.2019.258.

[38] Y. Xin et al., "Machine Learning and Deep Learning Methods for Cybersecurity," IEEE Access, vol. 6, no. c, pp. 35365–35381, 2018, doi: 10.1109/ACCESS.2018.2836950.

[39] F. Hutter, L. Kotthoff, and J. Vanschoren, Automated machine learning : methods, systems, challenges. 2019.

[40] O. Kováč, M. Kovalčík, P. Fecilak, and F. Jakab, "Learning module of non-periodic signal digitization using ATMega328 microcontroller," ICETA 2014 - 12th IEEE Int. Conf. Emerg. eLearning Technol. Appl. Proc., pp. 255–260, 2015, doi: 10.1109/ICETA.2014.7107594.

[41] N. Savitha and S. Malathi, "A Survey on Fire Safety Measures for Industry Safety Using IOT," Proc. 3rd Int. Conf. Commun. Electron. Syst. ICCES 2018, no. Icces, pp. 1199–1205, 2018, doi: 10.1109/CESYS.2018.8723930.

[42] C. P. Kruger, G. P. Hancke, and S. Networks, "Internet of Things Vision in wir. sensor net.," pp. 627–632.

[43] A. Jaber, F. Guarnieri, and J. L. Wybo, "Intelligent software agents for forest fire prevention and fighting," Saf. Sci., vol. 39, no. 1–2, pp. 3–17, 2001, doi: 10.1016/S0925-7535(01)00021-2.

[44] S. T. Grosser, "(12) United States Patent," vol. 2, no. 12, 2015.

[45] D. Tien Bui, Q. T. Bui, Q. P. Nguyen, B. Pradhan, H. Nampak, and P. T. Trinh, "A hybrid artificial intelligence approach using GIS-based neural-fuzzy inference system and particle swarm optimization for forest fire susceptibility modeling at a tropical area," Agric. For. Meteorol., vol. 233, pp. 32–44, 2017, doi: 10.1016/j.agrformet.2016.11.002.

[46] Google, "Dialog Flow." [Online]. Available: https://dialogflow.com.

[47] N. Benichou, A. H. Kashef, I. Reid, G. V. Hadjisophocleous, D. A. Torvi, and G. Morinville, "FIERAsystem: A fire risk assessment tool to evaluate fire safety in industrial buildings and large spaces," J. Fire Prot. Eng., vol. 15, no. 3, pp. 145–172, 2005, doi: 10.1177/1042391505049437.

[48] G. Chu and J. Sun, "Decision analysis on fire safety design based on evaluating building fire risk to life," Saf. Sci., vol. 46, no. 7, pp. 1125–1136, 2008, doi: 10.1016/j.ssci.2007.06.011.

[49] P. J. Moss, R. P. Dhakal, M. W. Bong, and A. H. Buchanan, "Design of steel portal frame buildings for fire safety," J. Constr. Steel Res., vol. 65, no. 5, pp. 1216–1224, 2009, doi: 10.1016/j.jcsr.2008.09.003.

[50] T. Davletshina, Industrial Fire Safety Guidebook. Elsevier, 1998.

[51] M. J. Hurley et al., SFPE handbook of fire protection engineering. Springer, 2015.

[52] N. S. Patil, N. Patil, P. Wani, S. Kolge, U. Keote, and K. Veer, "Fire Detection and Safety Navigation System using AI and IOT," pp. 6–10, 2019.

[53] P. K. and N. C. Vinay Dubey, Forest Fire Detection System Using IoT and Artificial Neural Network, vol. 55, no. January 2019. Springer Singapore, 2018.

[54] P. A. Rosas, Julio C´esar, Jos´e Alfonso Aguilar, Carolina Tripp-Barba, Roberto Espinosa, "A Mobile-Sensor Fire Prevention System Based on the Internet of Things," vol. 10409, no. October, pp. 338–353, 2017, doi: 10.1007/978-3-319-62407-5.

[55] J. Vera-Perez, D. Todoli-Ferrandis, V. Sempere-Payá, R. Ponce-Tortajada, G. Mujica, and J. Portilla, "Safety and Security oriented design for reliable Industrial IoT applications based on WSNs," IEEE Int. Conf. Emerg. Technol. Fact. Autom. ETFA, vol. 2019-Septe, pp. 1774–1781, 2019, doi: 10.1109/ETFA.2019.8869204.

[56] J. Zalewski, P. A. Laplante, and B. Amaba, "IoT Safety: State of the Art," IT Prof., vol. 21, no. 1, pp. 16–20, 2019, doi: 10.1109/MITP.2018.2883858.

[57] D. Deif and Y. Gadallah, "Reliable wireless sensor networks topology control for critical internet of things applications," IEEE Wirel. Commun. Netw. Conf. WCNC, vol. 2018-April, pp. 1–6, 2018, doi: 10.1109/WCNC.2018.8376992.

[58] B. Safaei, A. M. H. Monazzah, M. B. Bafroei, and A. Ejlali, "Reliability side-effects in Internet of Things application layer protocols," 2017 2nd Int. Conf. Syst. Reliab.

Safety, ICSRS 2017, vol. 2018-January, pp. 207–212, 2018,
doi: 10.1109/ICSRS.2017.8272822.