Enhancing Virtual Classroom Management for Sustainable Development: Qualitative Analysis

Julianah O. FALORE[1] & Afolakemi O. OREDEIN[2]

dunifalo6@gmail.com[1] a.oredein@lcu.edu.ng[2]

+234 802 319 1254[1] ; +234 805 514 5060[2]

Department of Arts and Social Science Education
Faculty of Education
Lead City University, Ibadan, Oyo State, Nigeria

This paper seeks to investigate how virtual classroom management can enhance sustainable development through a qualitative analysis. Simple sampling method was used to determine the study's population. The interview was conducted with 60 school administrators in the six stratified Education Districts in Lagos State, recorded, transcribed using Data Saturation The paper investigates current virtual classroom management strategies and identify gaps in implementation that can be address to improve sustainability. It then presents a series of case studies which illustrate how successful virtual classroom management strategies can be implemented and demonstrate how they can contribute to sustainable development. Evaluation of these case studies provides an analysis of the effectiveness of different virtual classroom management strategies and identifies the strength and weaknesses in each approach. The paper concludes with a set of recommendations for virtual classroom managers who seek to improve sustainability through their management practices. The findings of this paper will be valuable for virtual classroom managers as well as education policymakers, providing insights into how virtual classrooms can be managed in a more sustainable manner

Keywords: Virtual classroom management, sustainable development
Wordcount: 176

Introduction

In recent years, the integration of technology in education has witnessed a paradigm shift, with virtual classrooms emerging as a viable alternative to traditional face-to-face instruction. The advent of virtual classrooms has been catalysed by advancements in information and communication technologies, enabling educational institutions to reach a broader audience while overcoming geographical constraints and fostering more inclusive learning environments. However, the

successful implementation of virtual classrooms necessitates effective management practices to harness their full potential.

Virtual classroom management refers to the set of strategies, techniques, and tools employed by educators and institutions to facilitate a smooth and productive learning experience in the virtual setting Srisawat&Piriyasurawong, (2022). The planning approach, methodologies, tools, Apps and addressing students' attention. Ucar&Acar (2022) It encompasses various aspects, such as maintaining learner engagement, fostering collaboration among students, addressing technical challenges, and promoting an inclusive and equitable learning environment. Kesharav, Mirmoghtadale&Nayyeri (2020). Therefore, virtual classroom management is a tool that makes learning process inventive and flexible since it integrates information with learning innovations and modern technology in different ways. As virtual classrooms gain prominence, understanding and optimizing management strategies in this context have significant implications for the advancement of sustainable development in the education sector. Virtual classroom management can also be described as the strategies, techniques, and tools used by educators and institutions to effectively facilitate learning and maintain a productive virtual learning environment Mosteanu (2017). As the use of virtual classrooms continues to expand, particularly in response to the COVID-19 pandemic, understanding and implementing effective management practices such as a well- established curriculum, careful planning, monitoring of student's behaviour, and the utilization of technology resources specific to virtual classrooms are all necessary for effective class administration for ensuring successful online education.

For effective classroom management to take place in the teaching and learning process, there are some crucial elements that teachers must consider. One of the factors is that of engagement of interaction: Creating an engaging virtual classroom environment is crucial for keeping students actively involved in the learning process. Educators employ various techniques to promote student engagement, such as interactive discussions, multimedia presentations, real-time feedback, and collaborative activities. These strategies aim to foster interaction between students and the instructor, thereby enhancing learning outcomes.

Another element to be considered is establishing clear expectations and guidelines; Clearly communicating expectations and guidelines is essential in virtual classrooms to ensure that students understand their responsibilities, deadlines, and behavioural norms. Educators should provide students with a comprehensive syllabus, detailed assignment instructions, and a well-defined code of conduct. Setting clear expectations helps maintain discipline and creates a structured learning environment.

Furthermore, technical support is an important factor that cannot be glossed over; This is because the technical issues can disrupt the learning process in virtual classrooms. Providing technical support to students is vital to address any connectivity, software, or hardware-related

problems they may encounter. Educators and institutions should offer assistance and resources for troubleshooting common technical issues to minimize disruptions to the learning experience.

Moreover, there is need for building a sense of community: Establishing a sense of community in the virtual classroom is crucial for promoting collaboration, communication, and mutual support among students. Educators can foster this sense of community through icebreaker activities, group projects, virtual office hours, and discussion boards. Building a supportive learning community enhances student engagement and creates a more inclusive and participatory virtual learning environment.

The issue of monitoring and assessment is also significant: Regular monitoring of students' progress and timely assessment of their work are vital aspects of virtual classroom management. Educators can utilize a variety of assessment methods, including quizzes, projects, assignments, discussions, and examination, to evaluate student learning and provide feedback. Monitoring students' participation and progress allows educators to identify struggling students and provide additional support when needed.

Participants that are involved in virtual classroom must possess digital literacy and online etiquette: Developing students' digital literacy skills is essential for effective virtual classroom management. Educators should ensure that students are proficient in using the necessary technology tools and platforms for online learning. Additionally, promoting online etiquette, such as proper etiquette, respectful communication, and responsible digital behaviour, helps to maintain a positive and professional learning environment.

Inclusive practices should also be incorporated: Virtual classroom management should prioritize inclusivity and address the diverse needs of students. Educators should consider accessibility requirements, accommodate different learning styles, and provide alternative means of engagement for students who may face challenges in the online environment. Implementing inclusive practices ensures that all students can fully participate and benefit from virtual learning experiences. By effectively implementing these management strategies, educators can create engaging and productive virtual learning environments that support student learning, collaboration, and academic success. Additionally, virtual classroom management plays a significant role in promoting sustainable development in education by providing equitable access to quality education, reducing the carbon footprint associated with physical infrastructure, and fostering inclusivity and social equity.

Sustainable Development

Sustainable development is a guiding philosophy that attempts to achieve human develop objectives while allowing natural systems to support human needs for essential ecosystem services and natural resources. Virtual classroom management will go a long way in enhancing the realisation of the objectives of sustainable development. Development that satisfies current

situation and conditions without compromising the capacity of future generations to satisfy their own needs is referred to as sustainable development. Sustainable development according to United Nations (UN) declaration of 2005 World summit described sustainable development as the organizing principle for achieving human progress while maintaining the capacity of natural systems to supply the natural resources and ecosystem services that are essential to the economy and the society Ciegis, Ramanuskiene, & Martinkus (2009) argued that the economy, environment, and society are all interconnected. Rabie (2016) identified the simultaneous pursuit of environmental, qualitative, economic, human development, social equality, freedom, human values, and cultural as varieties that constitute sustainable development Sustainable development asks for engaging teaching methods that empower students to make decisions and change their behaviour in the interest of sustainability.

Sustainable development recognizes the interdependence between economic, social, and environmental dimensions and seeks to create a balanced and resilient society. The concept of sustainable development gained prominence with the publication of the Brundtland Report in 1987, which defined sustainable development as "development that meets the needs of the present without compromising the ability of future generations to meet their needs." It recognizes that economic development must be pursued in a way that protects and enhances social well-being and ensures environmental sustainability.

The environment, social equity and the economy are the three primary pillars of sustainability, there are three pillars are often known as “people, planet, purpose and profits”:

Environmental Sustainability focuses on preserving natural resources, minimizing pollution, and mitigating climate change. It involves practices such as sustainable land use, conservation of biodiversity, promotion of renewable energy, efficient resource management, and waste reduction. Also, social equity: Social equity emphasizes fair distribution of resources, opportunities, and benefits within society. It aims to address social inequalities, promote inclusivity, and ensure access to basic necessities such as education, healthcare, and livelihood opportunities for all individuals, regardless of their socio-economic background, gender, or other characteristics.

The importance of economic development cannot be over-emphasised while discussing sustainable development: Economic development seeks to promote long-term prosperity while considering the social and environmental impacts of economic activities. It involves fostering innovation, supporting responsible business practices, promoting sustainable consumption and production patterns, and creating economic opportunities that benefit society as a whole.

Sustainable development recognizes the interconnectedness of these dimensions and promotes a holistic and integrated approach to decision-making. It requires balancing short-term economic gains with long-term environmental and social considerations. Policies and strategies that support sustainable development often involve collaboration between governments,

businesses, civil society, and individuals to ensure collective action towards common goals. Education plays a vital role in advancing sustainable development by raising awareness, fostering critical thinking, and promoting sustainable practices (Baena-Morales, Merma-Molina, Ferriz-Valero 2023). It equips individuals with the knowledge, skills, and values necessary to contribute to sustainable development in their personal and professional lives. Education for sustainable development promotes environmental stewardship, social responsibility, and ethical behaviour Bascope. Perasso & Reiss, (2019).

In the context of education, sustainable development implies the integration of sustainable practices and principles into educational policies, curriculum, teaching methodologies, and learning environments. It involves incorporating sustainability themes, such as climate change, biodiversity, and social justice, into educational programs across various disciplines. Education for sustainable development aims to empower individuals to become active participants in creating a more sustainable and just world.

The achievement of sustainable development requires collaboration, innovation, and transformative actions at local, national, and global levels. Governments, businesses, institutions, and individuals must work together to address the challenges posed by unsustainable practices and promote sustainable solutions that balance economic growth, social equity, and environmental protection. By embracing sustainable development principles, societies can strive towards a future that meets the needs of the present generation while safeguarding the well-being of future generations.

Sustainable development in education aims to ensure that educational practices are economically viable, socially equitable, and environmentally responsible. By leveraging virtual classrooms, educational institutions can contribute to sustainability goals by reducing the carbon footprint associated with physical infrastructure and transportation, thus minimizing the impact on the environment. Moreover, virtual classrooms open up opportunities for students from diverse backgrounds, including those in remote and underserved areas, to access quality education, promoting social equity and inclusivity.

Numerous studies have explored the benefits and challenges of virtual classrooms and emphasized the importance of effective management practices in realizing their potential for sustainable development. According to researchers such as Akpan, Etim, & Ogechi (2016), wellstructured virtual classroom management positively influences students' engagement and academic performance, leading to higher satisfaction and retention rates. Additionally, research by Cannon (2019) emphasizes the significance of collaborative activities in virtual classrooms for enhancing students' critical thinking skills and fostering a sense of community among learners.

Despite these promising insights, there remain notable gaps in the existing literature. For instance, while some studies have explored the technical aspects of virtual classroom management, others have focused on pedagogical approaches. However, comprehensive research that examines

both technological and pedagogical dimensions in conjunction is scarce. Moreover, the impact of virtual classroom management on sustainable development outcomes remains a relatively unexplored area of research. Therefore, this study seeks to address these gaps by conducting a thorough investigation into the realm of virtual classroom management and its implications for sustainable development in education. By analysing the synergistic relationship between effective management practices and sustainable educational outcomes, this research aims to provide valuable insights for educators, policymakers, and stakeholders to optimize virtual learning environments for long-term sustainability and inclusivity.

Statement of the Problem

The incursion of COVID-19 into the world and advancement in technology has led to the upsurge in the use of virtual classroom in management secondary schools in Lagos state just like in other educational institution all over the globe. Despite this laudable development, many teachers and students are not maximising the opportunity to teach and learn judiciously. Many teachers do not know how to manage the class effectively. Most students seem to have challenges in order to access the new virtual classroom. Therefore, this research endeavour to bridge the gap by investigating how virtual classroom management can enhance sustainable development.

Aim and Objectives

The aim is to investigate virtual classroom management and its implications for sustainable development. The objectives are to:

i. identify the most virtual classroom platforms for teaching secondary school students in Lagos State ii. identify the challenges encountered by using virtual classroom management in teaching secondary schools' students in Lagos State

iii. identify the rules guiding the virtual classroom platforms in secondary schools in Lagos State

iv. analyse ways in which virtual learning sustain education especially in secondary schools in Lagos State

Research Questions

The following research questions guided the study.

1. What are the virtual learning platforms used for teaching and learning in Lagos State during COVID-19 and what is the mostly commonly used virtual platforms.
2. What are the challenges faced by the teachers in secondary schools using virtual learning platforms in Lagos State.
3. What are the rules guiding the virtual learning platforms in secondary schools in Lagos State?
4. How can virtual learning sustain education in secondary school?

Methodology

Research Design

In this research, empirical qualitative methodology was used to collect the data from respondents to determine teachers experiences on virtual classroom management and sustainable development. 60 administrators were interviewed in a semi- structured fashion to gather data. The respondents were chosen randomly from the six districts that makes up the twenty local government in Lagos state; Agege, Ikorodu, Lagos Island, Lagos Mainland, Ajeromi- Ifelodun and Oshodi – Isolo. The interview was recorded and transcribed using data saturation The interview questions consist of four semi- structured questions

Results and Discussion of Findings

Virtual Learning Platforms

The following learning platforms were mentioned by the respondents as being utilized for learning; goggle meet (5), zoom (3), Learning Management System (3), Telegram, and WhatsApp (41), Radio (10), Television (8). Questions about why teachers used some specific platforms from the ones listed. The responses differ; while private schools used goggle meet, zoom, LSM and WhatsApp, public schools used Radio, Television, and WhatsApp however, WhatsApp was the most preferred because of its effectiveness and easy to use which allows sharing of audio lesson and recording of lessons.

Q1*:* What are the virtual learning platforms used and the most commonly platform used for teaching and learning during COVID-19?

Respondent: 1 *There are now more opportunities for teaching and learning. Thanks to virtual learning platforms. Students were enthusiastic as a result of having access to the platforms since it made learning more participatory and exciting. Despite this, there were variety of outlets used in my school including zoom, goggle meet, Radio, Television and Telegram. WhatsApp was primarily used.* Respondent: 2 *The lock down was not really what we anticipated. My school initially used Radio and Television introduced by the Lagos state government to continue their studies, having realized that there was no way they could keep an eye on the students as regards the level of student's involvement in listening to Radio and Television program, we switched to WhatsApp which was commonly used by teachers and students.*

Challenges faced by Teachers

The interviewees agreed that teachers faced a variety of difficulties including; inadequate preparation and lack of technology know- how on the part of the teachers; resistance to change; discipline difficult to instil in students; poor electricity; poor internet connections; difficulty in managing time; students not being punctual at classes; lack of a conducive environment to learning, lack of student's access to technology, and students' misbehaviour.

Q2: What are the challenges faced by the teacher in using virtual learning platforms?

Respondent: 1 *The challenges faced by teachers were numerous among which were; students lack of access to Android phone, no data, poor power supply; distractions or unexpected noise at the background from the family, friends and pets that diverted students' attention and participation during virtual teaching; parents were thus contacted to provide a conducive environment that would allow their wards to be focused when classes were in progress.*

Respondent: 2 *Before the outbreak, many teachers exclusively used WhatsApp to communicate with their friends and family only, using WhatsApp to educate students presented a significant difficulty for teachers, many students lacked the tools to use in order to participate in the virtual learning teaching this made it impossible for them to receive education, students not attending classes on time and inability of teachers to discipline and to keep track of student's participation in learning*.

Virtual Classroom Management

Teachers were unable to fully police the rules governing the virtual learning platforms, according to the responses from the respondents, it is a novel phenomenon and a challenging duty for teachers to monitor students' behaviour, uphold order and control, and keep students' attention throughout virtual learning platforms. WhatsApp was the medium that students in Lagos State mostly utilized for instructions and communication, however, this excludes students who do not have smartphones or who could not afford buying data to miss classes. At times when teachers were available on line, few students showed up, in some situations, classes were rescheduled to accommodate this, making it impossible to enforce discipline.

Q3 What are the rules guiding the virtual classroom platform?

Respondent: 1 *Our school established guidelines for students to follow while participating in virtual learning; these include adhering to the scheduled timetable, being punctual and marking attendance as soon as they join the platform, refraining from sending messages that are not related to the goal of forming the group, and turning off their cell phones when not in use*.

When compared to physical classes, the majority of the regulations, however, were not followed because; the used of WhatsApp platform for learning was new in the educational system

in Nigeria, the platform does not entail one-on-one interactions, thus making it difficult for teachers to manage their classes

Respondent*: 2 The school established rules that students must follow when using virtual instructions. These include being on time, staying on the platform until the session was finished, turning down their speakers, submitting assignments on time, avoiding distractions and refraining from using foul language*.

Teachers must be patient and cautious when dealing with such unethical activities, and the rules governing the platform should always be forwarded before the start of the class to serve as a reminder to students. Controlling unethical behaviour among students online is a serious issue for teachers to maintain effective virtual classroom management.

Virtual Learning and Sustainable Education

Globalisation impacted how education plays a part in development for internal competition among nations for information- based goods and services, knowledge and skills have become more crucial for economic progress. Lifelong learning incorporates learning objectives, content pedagogy, learning environments and enhancements to the cognitive, socio-emotional and behavioural components of learning.

Q4: How can virtual learning sustain education in secondary school?

Respondent: 1 *Virtual learning raised our students' knowledge of the -use of technology and exposes them to the world of teaching and learning which is crucial for the long-term improvement in education. As you are aware, the use of virtual learning has reduced the need for community and transportation. Thus, a student can access learning from home.*

Virtual learning is used to prepare future generation through their exposure to technology, it thus supports educational progress by producing leaders who can work to address problems in local and global communities.

Respondent :2*: Students in my school had access to laptops and Android phones, enabling them to receive an education regardless of where they were born and their gender. In addition to this, they connect with students, help them to form a network, and as they advance with everyday applications*

Making critical decision and evaluating the reliability of the information they are exposed to while navigating information and allow students to maintain their abilities current in a constantly changing world, preparing them for modern workplace

Research Question 1: What are the virtual learning platforms used for teaching and learning during COVID-19 in secondary schools in Lagos State and what is the mostly commonly used virtual platform?

Based on the responses from the school principals, the virtual learning platforms used for teaching and learning during COVID-19 included a variety of options, such as Zoom, Google Meet, Radio, Television, Telegram and WhatsApp. WhatsApp was the most commonly used platform for teaching and learning.

Discussion of Findings

Research Question One: The responses highlight the diverse range of virtual learning platforms adopted during the COVID-19 pandemic in Lagos State. Its evident that schools explored different options to facilitate remote education and maintain continuity in learning. The platforms mentioned, such as Zoom, Google Meet, Radio, Television, Telegram, and WhatsApp, have their unique features and advantages for virtual teaching and learning. WhatsApp emerged as the most commonly used platforms in schools. This aligns with the general trend observed during the pandemic, where WhatsApp gained popularity for educational purposes due to its widespread use, ease of accessibility, and familiarity among students and teachers. This finding aligns with that of Selvaraj, Vishru, Benson, KA, and Mathew (2021) where WhatsApp was the most preferred platform (68%) as they are easy to handle and do not require any technical skills for operating, especially by school students. Similarly, another study conducted by Ratminingsih, Adi Ana, Fatmawan, Artini, and Padmadewi (2022) revealed that students had a highly positive opinion of using WhatsApp. They resoundingly concurred that it facilitated better oral and written communication skills and was convenient to utilize during the COVID-19 pandemic. Through discussion exercises that were undertaken both before and during learning process, students also acknowledged that it improved their critical thinking. As a result, it improved their comprehension of the instructional content resources., internet accessibility, and the level of digital literacy among students and teachers. Additionally, Lagos State government-initiated Radio and Television programs to support remote education. The use of Radio and Television programs reflects an approach taken in some regions to reach to students who may not have access to the internet or suitable devices. Theses initiatives were implemented indifferent countries to ensure educational continuity during the pandemic.

Research Question 2: What are the challenges faced by teachers in using virtual classroom platforms in secondary schools in Lagos State?

Findings

During the shift to online learning, teachers faced a variety of challenges that hindered the efficiency of these platforms. One significant problem was the lack of training and technological ignorance of certain teachers, which made it challenging for them to effortlessly incorporate technology into their teaching methods. Additionally, their capacity to adjust to the new virtual platforms was hampered by a lack of familiarity with technology-based education and an aversion to change. Another big challenge was how to maintain discipline in the virtual environment. Students' attention and active engagement during virtual classes were impaired because they frequently encountered background distractions from family, friends, or pets which led to a less concentrated learning environment. This lack of suitable environment negatively affected their learning experience and overall academic performance. Infrastructure problems also made the situation worse. Both teaches and students were impacted by the insufficient electrical supply and the unstable internet connectivity. Time management also became a top priority

Discussion of Findings

The results show that teaches faced a variety of difficulties when they made the switch to virtual learning, including those related to teacher readiness and digital literacy, infrastructure and technology accessibility, student engagement and behaviour management, and time management. These difficulties include both instructional issues and technical difficulties. The results of this study are consistent with those of Mardiani and Azhar (2021), who found that the teacher faced numerous difficulties in the virtual classroom teaching, including the students lack of readiness to enroll, an internet connection issue, a time constraint that forced the teacher to start teaching the essentials right away, students turn-off of the camera and sound, students inattentive to learning, a lack of interaction and ineffective management. From the viewpoints of the teacher and the students Biwas and Nandi (2020) recognized internal as subjective and external as objective challenges. Anwar, Khan and Sultan (2020) identify teachers' unpreparedness to accept the change towards digitalization due to their lack of necessary resources and abilities.

Research Question 3: What are the rules guiding the virtual learning platforms in secondary schools in Lagos State**?**

Findings

Based on the responses from the school principals, the rules guiding the virtual learning platforms were as follows

Respondents: The school established rules for students to abide by during virtual learning, including sticking to the set timetable, showing up on time, marking attendance promptly after logging on to the platform, refraining from sending irrelevant messages in the virtual group, and

turning off cell phones when not in use. The result shows that many of the recommendations were not strictly followed, nevertheless, perhaps as a result of WhatsApp's novelty as a teaching tool in Nigeria. It was claimed that the platform lacked one-on-one contact made it difficult for teachers to successfully monitor their classrooms. In addition, students were to remaining on the platform until the session was finished, mute speakers to reduce distractions, turning in assignments on time

Discussion of Findings

The results highlight the efforts made by schools to set standards and regulations for online learning environments. These guidelines seek to preserve harmony, order, and productive learning environments Enforcing these standards, however was difficult due to the unique nature of virtual learning and in particular platform employed (WhatsApp)The guidelines in this study are consistent with Abubaker's findings from 2023, who offered various suggestions for techniques teachers might utilize to deal with the challenges of managing classrooms .Al-Hawamleh, Alazemi,.Dina, Al-Jamal, Al Shdaifat and Gashti (2022)identified three learning guides for online teaching; teachers are to analyze the task requirements, create productive goals and select appropriate activities that concentrate on the integration of conceptualization of new topics in accordance with learning guides. This will make students to feel less anxious and reserved

Research Question 4: How can virtual learning sustain education in secondary schools?

Findings

Based on the responses from the school principals, they identified so many ways in which virtual learning can sustain education in secondary schools.

Discussions of Findings

The results show how virtual learning can support secondary school education by encouraging technology integration, which is a cutting -edge approach to teaching and learning that improves students' technological literacy and usage. A culture of lifelong learning is promoted by improved access to education, which lowers barriers to education, enables students to access learning regardless of their location gender, and skill development among students that encourages them to navigate and critically evaluate information. The conclusion of this study is consistent with those Klanja-Milicevic and Ivanovics research on sustainable education and e-learning (2021). Similarly, SERIN (2020) found that most teachers find virtual reality to be intriguing and that it motivates students to engage in learning

Conclusion

By offering a productive learning environment for the development of the competence required to engage effectively, virtual learning has the potential to support sustainable development. The study

also addressed the difficulties teachers encounter while using virtual learning. The results from the interviewees revealed that teachers had difficulties when utilizing virtual learning platforms such as; environment not favourable to learning, students exhibiting bad behaviours, and students' non-attentiveness. To effectively manage the class, teachers must maintain outstanding classroom management. Some of these difficulties can be overcome by teachers, if they arrive on time for classes even before the students arrive, discipline disruptive students, make learning enjoyable, manage the lesson, make changes as needed, assign homework and provide links for students to conduct further research. The research's findings also indicate that there were a number of issues with virtual learning platforms for which administrators and teachers must have expertise in virtual classroom management in order to prepare for upcoming incident in the nearest future. Furthermore, the paper highlighted the most often used platforms for influencing knowledge during COVID-19 in Lagos State secondary schools. In conclusion, this article highlights the importance of virtual learning for promoting sustainable development which will be more significant for students, government, and stakeholders.

Recommendation

The recommendations below can be offered in line with the findings of this research.

1. Government should raise its spending on education while putting a strong emphasis on technology. Solar electricity will be provided to schools so that students can use virtual learning platform.
2. Parents should provide their wards with the gadgets needed for use during virtual learning teaching
3. Training teachers to keep them current on technological developments so that they can think creatively, and use methods to transfer knowledge to students to support sustainable development
4. Establishing partnerships between the government and business stakeholders will allow.it to acquire finances for students to have equal access to education and achieve SDG 4;1(UNESCO, 15)
5. Technology must be used to advance peace and justice through education by allowing for flexible learning, teachers professional development, students to have access to limitless resources and teachers to receive immediate feedback.

References

Abubaker, K.A, (2023). Challenges that Libyan primary school teachers faced in managing virtual classes, *The Online Journal of New Horizons in* Education, 13@) 73-79

Akpan, S. J., Etim. P.J., & Ogechi. U. S. (2016), Virtual classroom instructions and academic performance of educational technology students in distance education Enugu, *Online World Journal* https;//dx.doi.org/10.5430/wjev6n6p83

Anwar, M., Khan, A., & Sultan, K. (2020) The barriers and challenges faced by students in online education during COVID-19 pandemic in Pakistan Gomal Univ. J.Res. 36, 52-62

Al-Hawamleh, M.S., Alazemi, A.F., Al-Jamal, H.,Dina, A., Al Shadifat, S, &Gashti, Z. R(2022) Online learning and self- regulations strategies: Learning guide matters. *Journal of Education Research International* https://doi.org/10.1155/2022/4175854

Baena- Morales. S., Merma-Molina. G., &Ferriz-Valero (2023), Integrating education for sustainable development in physical education: fostering critical and systemic thinking. International Journal of Sustainability in Higher Education. https;//doi.org/10.1108/IJSHE10-2022-0343.

Bascope. M., Perasso. P., &Reiss, K (2019) Systematic review of education for sustainable development at an early stage: Cornerstones and pedagogical approaches for teachers' professional development Journal **Sustainability** https;//doi.org/10.3390/su11030719

Biwas, R. A., &Nandi, S., (2020). Teaching in virtual classroom: challenges and opportunities, *International Journal of Engineering Applied Sciences and* Technology, 5(!) 334-337

Bruthland Report of 1987 on world commission on environment and development' 'Our common future "chapter 2 https; www.un-document.net/ocf-02.htm

Cannon. A (2019*) Essential skills and collaboration-Technology and the curriculum https;//pressbooks.pub*

Ciegis, R. Ramanauskiene, *J. &*Martinkus *(2009), B. The concept of sustainable development and its use for sustainability scenarios 2(62) 3-11*

Kesharav K. Mirmoghtadale *Z.&*Nayyeri. S. *(2022*) Design and validation of the virtual classroom management questionnaire. *International Review of Research in Open and Distributed Learning*23(2) 1-14.

Klsnja-Mili'ceviç, A., Ivanovic (2021), M. E-learning Personalization Systems and Sustainable Education. Sustainability 2021, 13, 6713.

Liang, W. A& Fung, D. (2021). Fostering critical thinking in English- as-a second-language classroom: Challenges and opportunities. Thinking Skills and Creativity, 39, 100769

Mazumber, Q. H., Sultana, S., &Mazumber, F. (2020). Correlation between classroom engagement and academic performance of Engineering students. *International Journal of Higher Education.* 9(3), 240 https//doi.org/10.5430/ijhe. v9n3p240

Mosteanu. N.R(2020) Digital university campus- change education system approach to meet the 21st century needs. *European Journal of Human Resource Management Studies* 4(4) http;//www./oapub.org/soc 80-91

Mardiani. R, &Azhar. R. N. (2021). Overcoming challenges in virtual classroom to maintain effective classroom management and classroom culture: A case study at one vocational school. *Journal Samurasun Interdisciplinary Studies for Cultural* Heritage.07(02) 2021

Rabie.M.(2016) Meaning of sustainable development in a book; A Theory of sociocultural and Economic development DOI;10;1007/978-1-137-57952-23

Ratminigsih, M., Adi-Ana, K, T., Fatmawan, R., Artini, P., &Padmadewi, N., (2022) WhatsApp implementation on pedagogical content courses during COVID-19 pandemic: students learning activities and perception. *Kasetsart Journal* of *Social Sciences*,3(1) 238-244 htpps://doi.org/10 .34044/j.kjss.2022. 43. 1.32

Selvaraj, A., Vishnu, R., KA, N., Benson, N., Mathew (2021), A. Effect of pandemic based online education on teaching and learning system. *International Journal of Educational* Development,85,2021.102444, ISSN,07380593https://doi.org/10.1016/j.ijedudev.2021. 102444

Serin,H (2020). Virtual reality in education from the perspective of teachers. Artificial Intelligence, 9(26) 291-303. https://doi.org/10.34069/ai/2020.26.02.33

Srisawat, S, & Piriyasurawong, P, (2022), Metaverse virtual learning management Based on Gamification Model to enhance total experience**.** *International Education students archive* 15(5)

Ucar. R. & Azar. C. (2022) Virtual classroom management experiences of teachers. *International Journal and Education Psychology and Education Studies.* https;//ds.doi.org/10.52380/ ijpes. 2022.9.4.903

Unparking Sustainable Development Goal 4 Education 2030 Guide https://www. right-to-edn.org. / sites/right-to-edn.org/files/resource attached/

Tey, Y.S. & Brindal, M (2020). Sustainability stewardship: Does roundtable on sustainable palm oil certification create shareholder value? Corporate Social Responsibility and Environmental Management, 28 (2), 786-795. https://doi.org.10.1002/csr.2088

Enhancing Internet of Things Security Using Artificial Intelligence: A Structured Review

[1]Chekwube EZECHI & [2]Wilson SAKPERE

Department of Computer Science, Lead City University Ibadan, Nigeria
[1]zechirayjr@yahoo.com,
+234 802 811 6377

With the rapid growth of IoT, there are increasing security challenges such as hacking and data theft. Protecting the security and privacy of IoT networks becomes more complex as the number of interconnected devices rises. This paper investigates the potential of artificial intelligence (AI) in enhancing the security of Internet of Things (IoT) systems. The objectives are to identify the specific security challenges in IoT, examine AI-based solutions for IoT security, assess their effectiveness, highlight limitations, and propose future research areas. The study categorizes existing research based on AI techniques, including machine learning, deep learning, and natural language processing. It examines different AI-based approaches and methodologies, discussing their strengths, limitations, and real-world implementations. A literature review was conducted using prominent databases to gather insights on IoT security challenges and AI applications, such as anomaly detection and authentication. The review demonstrates that AI shows promise in addressing security challenges in IoT, including device identification, denial-of-service attacks, intrusion detection, and malware detection. However, further research is required to overcome limitations and challenges such as scalability, interpretability, resource constraints, and vulnerabilities to sophisticated attacks. Despite the challenges, AI-based IoT security solutions offer significant benefits in improving the security and reliability of IoT systems. By addressing the unique security challenges, AI can contribute to the creation of more secure and trustworthy IoT environments. The paper concludes by suggesting future research directions and strategies to integrate AI into IoT security frameworks, with the goal of building a secure and resilient IoT ecosystem.

Keywords: Internet of Things (IoT), Security, Artificial Intelligence (AI), Anomaly Detection, Denial-of-Service.

1. INTRODUCTION

In today's interconnected world, networks and communications technologies form the backbone of our modern society, powering everything from internet connectivity to mobile communications, cloud computing, and more. Networks and communications play a crucial role in connecting

people, devices, and systems, enabling the exchange of information, and facilitating collaboration on a global scale. A rapidly growing field, driven by the increasing demand for connectivity and the growth of the Internet of Things (IoT). As the number of devices connected to the Internet continues to grow, the need for secure, reliable, and efficient networks will become even more important.

The International Telecommunication Union formally proposed the concept of "Internet of Things" at the World Summit on the Information Society (WSIS) in 2005 (ITU Internet Reports, 2005). The term "Internet of Things" (IoT) describes a distributed network that connects various sensor devices and systems, including sensor networks, radio frequency identification (RFID) devices, barcode and quick response (QR) code devices, global positioning systems (GPS), etc. with the Internet using wired and wireless communication technologies, allowing embedded systems to interact and communicate (Hai-ming, 2010). The plethora of IoT services and applications span various industries, including manufacturing, energy management (using smart grids), urban living (using smart cities), and personal healthcare. IoT has steadily developed into a set of solutions for specific applications due to technological advancements and the growth of application domains.

The Internet of Things (IoT), which connects the physical world to the Internet and enables intelligent interaction, is focused on integrating and innovating solutions. The following three technology paths have always been followed in IoT development:

- The invention of sensing, identification, and authentication technologies that serve as IoT's foundations.
- The invention of transmission and communication technologies, which are essential to the Internet of Things because they will make it easier, more dependable, and safer to send and aggregate the vast amounts of data that IoT devices will collect to the processing unit or the central node.
- The invention of data processing and computing technologies, which are crucial for offering IoT data-based applications and services, as well as being the key to enhancing processing effectiveness and intelligence.

IoT typically has an entity-based architecture that can divide IoT from bottom to top into three layers, namely the terminal perception layer, network transport layer, and application service layer. This is in accordance with the complete information creation, transmission, and processing cycle, which takes into account the traditional architecture (Zhong et al., 2015) and the ISO/IEC 30141:2018 "IoT Reference Architecture" (Bauer et al., 2013, pp 163-221). In Figure 1 below, the precise architecture is displayed. This design unifies diverse IoT participants and demonstrates their interactive relationship with one another.

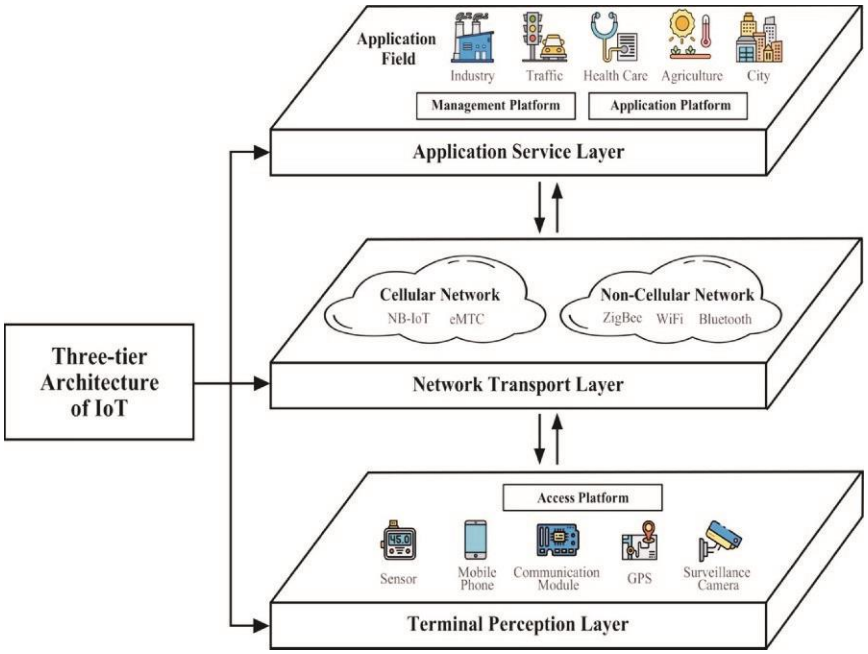

Figure 1. IoT Reference Architecture (Bauer et al., 2013). The three-tier architecture of IoT.

The terminal perception layer includes physical entities that represent real things, IoT device entities (sensor devices, RFID-enabled identification devices, and GPS-enabled positioning and tracking devices), and access platforms connecting local and wide area networks of IoT devices.

To implement the communication and connection functions, the network transport layer transports data from the terminal perception layer to the application service layer. For data encoding, authentication, and transmission, the network transport layer uses cellular networks (eMTC, NBIoT, etc.) as well as non-cellular networks (Wi-Fi, Bluetooth, ZigBee etc.).

The application service layer processes the data sent from the network transport layer and integrates it with different industries to support vertical IoT applications. It offers rich and specialized services for various users in various fields, such as smart grids, smart homes, and smart cities. The application service layer also consists of application & service subsystems that offer data storage, analysis, and service capabilities as well as operation maintenance & management subsystems that offer management and operation support capabilities.

2. Security Threats in Iot Layers

IoT has developed thanks to its widespread acceptance and extensive deployment, but these factors have also brought about new security risks. Its security maintenance is a difficult and demanding task. IoT security issues are becoming more and more problematic for the following reasons:

A. Terminal Perception Layer Security Threats

The terminal system's main components are sensors. Their primary job is to gather data while continuously monitoring objects. These tiny physical devices are widespread throughout several related engineering disciplines and are quite many. Since the majority of them are resource-constrained, attackers could potentially target them. The following security risks that exist for them are:

- **The first issue with the terminal perception layer is the device's unanticipated physical attack (Deogirikar & Vidhate, 2017).** Despite being valuable assets, IoT devices are frequently unsupervised. The connection between the devices and the central server is destroyed by criminals via theft, bodily harm, and other means. For instance, Chinese sharing economy businesses (such as those that rent out bicycles and portable chargers) experienced significant losses or even declared bankruptcy in 2018. The loss of assets caused by the violent removal of smart locks and location devices on bicycles and chargers accounts for a substantial portion of the cause.
- **During the information transmission of IoT nodes, there is a risk of attack.** Nodes in the terminal perception layer can be categorized into three groups: information aggregation nodes, isolated nodes, and collection endpoints. The information aggregation node is a server that is in charge of receiving, processing, and forwarding information; the isolation node is embedded equipment that is in charge of information encryption and decryption, as well as internal and external network isolation. The collection endpoint primarily corresponds to sensors, which are responsible for sensing and gathering information. Due to the transmission distance, there are risks associated with information connectivity between nodes, including interception, eavesdropping, forgery, and node tampering.
- **IoT device secure communication requires identification and authentication technologies, which are necessary pre-requisites (Chuankan et al., 2017).** IoT device security can be effectively increased by the uniqueness and certainty of identity, however, there are some ways for hackers to circumvent this process and carry out intrusion. For instance, iLnkP2P, a piece of software, was exposed in April 2019 without any authentication or encryption safeguards. With certain serial numbers, attackers can directly connect to IoT devices, get around the firewall, and send malicious messages in place of any legitimate ones the device might send.

B. Network Layer Security Threats

To create a vast network, IoT combines communication networks and sensor networks (Yick et al., 2008). The likelihood of attacks likewise rises sharply with the expansion of the network scale, much like the dangers posed to the terminal sensory layer. They face the following security risks:

- **The network's availability, integrity, and confidentiality are targeted by attackers on the network transport layer (Coss, 2014).** Some network targets are poorly protected, which makes it simpler for intruders to enter. A lack of protection and verification procedures allows an attacker to tamper with the platform's software and hardware, which increases the chance of stored data leakage. To prevent assaults and safeguard network security in the early stages, fast intrusion detection is essential.
- **Attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) will affect the network transport layer.** Attackers initiate DoS and DDoS attacks by providing traffic that is larger than the target's processing capacity to exhaust the target's network and computing resources, producing network blockage and a denial of service. DoS and DDoS attacks on a large scale will have severe effects on the entire network. Over 100,000 IoT devices were infected as a result of a large-scale DDoS attack carried out by Mirai, the botnet that first surfaced in 2016 (Kolias et al., 2017).
- **IoT's use of communication technologies has limitations**. IoT utilizes a variety of communication technologies (Al-Sarawi et al., 2017), including short and long-distance networks (ZigBee (Gislason, 2008), Wi-Fi, etc.), as well as the Internet. These technologies' security flaws have been carried over into IoT. For instance, the Internet offers a variety of services to various users, including IoT users, but at the same time, the TCP/IP-based communication infrastructure faces challenges like high complexity, poor scalability, and insufficient resource utilization (Al-Garadi et al., 2020). These threats include intrusion, replay attacks, and identity theft.

C. Application Service Layer Security Threats

In accordance with user needs, the application service layer processes the data transmitted from the network transport layer and offers services for various application situations. Through web applications or mobile apps, users can directly take advantage of the services offered by IoT systems and enjoy the convenience they bring. However, application-level attackers will cause issues with software, data, and system security respectively.

Software Security: Software attackers frequently utilize malicious programs. For instance, the Bank of Russia discovered in 2017 that the ATM malware *Bespalova*, which automatically paid after entering a specific code, was present. The system will be open to attacks from malicious scripts or error messages if there aren't enough code checks and testing. According to Bisht and Venkatakrishnan (2008), attackers might employ XSS (Cross-Site Scripting) Attack to insert harmful code into a different reliable website, for instance. Successful XSS attacks have the potential to take over IoT accounts and render the IoT system inoperable. Additionally, the prevalence of Android malware has significantly grown recently (Faruki et al., 2015). Android

mobile operating system openness has assisted in malware propagation on mobile devices. Malware can infiltrate mobile devices and steal confidential data.

Data Security: SQL injection, privilege promotion, and backup theft are common database threats **(Dorai & Kannan, 2011)**. The application service layer has a security requirement that data privacy be protected. Numerous IoT data points, like GPS-derived position data, may contain personally identifiable information. Attackers may utilize such data to examine sensitive personal information about users, including their address, income, way of life, behaviour, and state of health (Jing et al., 2014)

System Security: The application service layer is made up of fundamental environments, parts, and virtualized cloud infrastructure. Attackers will utilize fundamental settings and elements, such as operating systems, databases, and middleware, to conduct man-in-the-middle and brute-force attacks, leading to unauthorized access, remote control, and data leaking. To lower equipment deployment costs and increase computing performance or business throughput, the majority of IoT systems create virtualized cloud platforms. However, the use of virtualization technology also entails security risks, which can result in issues like virtual machine escape, virtual network attacks, and vulnerabilities in virtualized software.

3. Application of Ai to Iot Security: A Feasibility Analysis

A. IoT Security: Common Characteristics and Special Requirements

The examination of different IoT security issues has revealed several common traits, which make IoT security more complicated and result in unique security protection requirements that are distinct from those of other areas. The common characteristics are as follows;

- **In a normal IoT context, the distribution of data stays relatively stable, making the identification of abnormal behaviours and data outliers the main IoT security requirement.**The majority of IoT devices can only perform basic activities like data gathering and data transmission due to a lack of resources. Both the acquired data and the vast majority of popular gadgets will continue to operate in their regular modes. In the case of consumer IoT devices, for instance, the network traffic typically follows regular patterns. In order to make their network operations more predictable and organized, these devices frequently deliver steady signals to a small number of endpoints (Doshi et al., 2018). The network traffic generated by DoS/DDoS assaults, on the other hand, will be very different from that produced by IoT devices. As a result, effective defences against many security assaults include real-time monitoring, abnormal data detection, prompt capture, and early notification of abnormal business data flow. The fundamental necessity for IoT security is to find solutions that can effectively differentiate between normal and abnormal modes.

- **Lack of prior knowledge results from the unpredictable and variable nature of attack modes, which raises the bar for the robustness and generalizability of security protection models.** When it comes to personal privacy, there has historically been a risk to information security. IoT attack scenarios, however, also exhibit a trend of diversification as the IoT sector grows in size. Attacks on communication interfaces, cloud platforms, and hardware and software vulnerabilities are constantly developing. Defenders can't quickly implement the right countermeasures because they lack prior knowledge about new attack tactics (Madaan et al., 2018). Users now pose a far greater security risk because they can only comprehend the attack after experiencing loss. Security models must be able to maintain their efficacy in a variety of unanticipated circumstances if there is insufficient prior knowledge, which calls for greater resilience, generalization capability, and data control capability.
- **Low-power devices' and microservice terminals' security mechanisms are incapable of automatically protecting, learning, and upgrading themselves.** Complex security techniques cannot be used due to the large-scale interconnection of IoT devices, which necessitates low-power and low-cost solutions. As a result, it is challenging for current IoT security protection approaches to update out-of-date security techniques. The majority of them lack the capacity for self-renewal and evolution, which puts them far from what is known as "active immunity" or "auto-immunity" (Riahi et al., 2013). These techniques rely on humans to maintain and update the database, define new attack modes, and establish interception rules because they lack initiative. When there is a lot of manual involvement, security protection lags somewhat and cannot quickly learn and upgrade the security scheme.
- **The integrity of IoT requires security schemes to be capable of effectively handling massive data and can be deployed in a large-scale and unified manner.** The Internet of Things (IoT) is a multi-layer system that spans terminals, networks, and service platforms. Security concerns are defended holistically, and data are more sophisticated and extensive. The IoT's unity and integrity present an urgent need for security solutions that can process massive amounts of data, and it's important to make sure that these solutions can be uniformly deployed in a large-scale manner, remain effective in challenging circumstances, and evolve in response to new situations at any time.

B. AI's New Capabilities for IoT Security

New security technologies are desperately needed because of the uniqueness of IoT security and the shortcomings of conventional approaches. Artificial intelligence has several potential applications as a new field of technology (Mahdavinejad et al., 2018). Artificial intelligence (AI) researchers are primarily interested in machine learning (ML). Its theory and techniques have been extensively employed to resolve challenging issues in numerous engineering applications. There

are two types of ML algorithms used for IoT security: transaction algorithms and decision algorithms.
(See Figure. 2).

Data preprocessing and data exploration are mostly handled by transaction algorithms. Decision algorithms are built on the foundation of transaction algorithms, which use a small number of samples and straightforward models to determine the basic properties of the dataset. The majority of business decisions are made by decision algorithms, which use a variety of decision-making techniques to lower the likelihood of error and maximize overall profit. Three categories of decision algorithms which are single decision-making, sequential decision-making, and integrated decisionmaking can be distinguished based on approaches and situations.

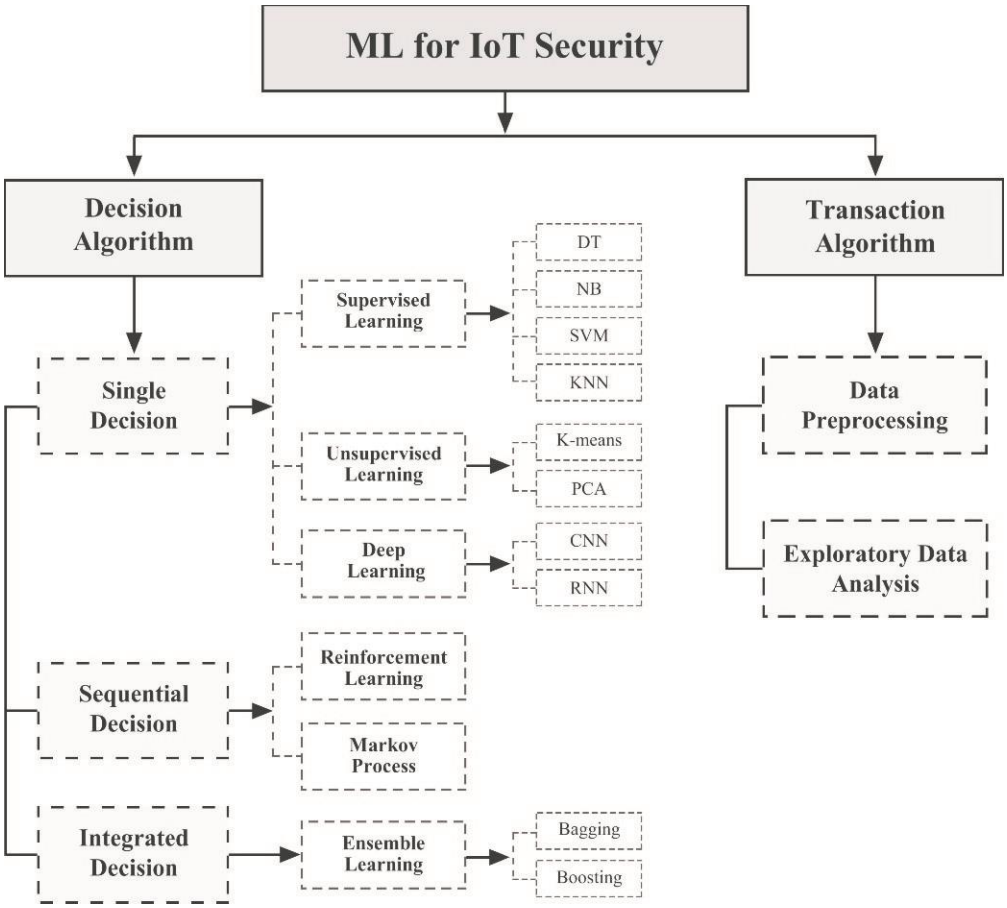

Figure 2: Machine learning for IoT security. (Wu et al., 2020)

The ability of pattern recognition and abnormal behaviour discrimination: We know that the business modes of IoT devices are fixed, and their typical actions are predictable and structured thanks to the analysis of the majority of IoT security events. ML techniques like supervised learning and unsupervised learning can offer strong abilities to record abnormal actions and detect abnormal patterns, allowing for the classification of normal behaviours and abnormal attacks. Therefore, both supervised learning and unsupervised learning have a wide range of applications in IoT security. For instance, one particular idea is to utilize Support Vector Machine (SVM) (Liang, 2015), a supervised learning technique, to determine whether an access device is approved. To classify different devices and stop unauthorized devices from being used, SVM can utilize a hyperplane to partition points in the feature space of device data into two categories: blue nodes are authorized devices, and yellow nodes are unauthorized devices (as illustrated in Figure. 3).

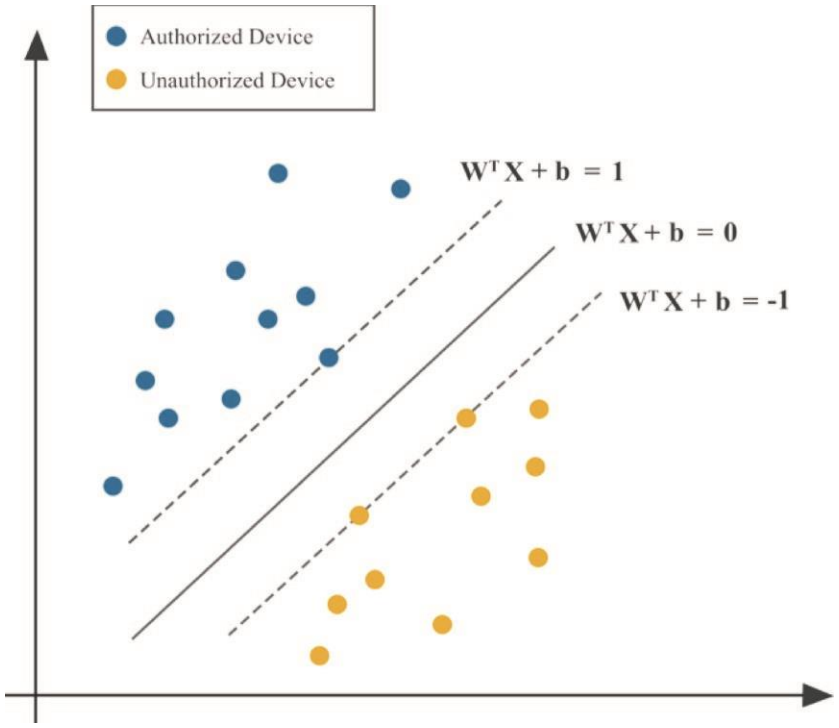

Figure 3. An example of IoT devices classification based on SVM (Liang, 2015)

✍The ability to autonomously protect, learn, and update: One of the key factors limiting the practical applicability of classic schemes is a lack of learning and upgrading capabilities in uncharted situations. Traditional security measures are ill-equipped to deal with new viruses or attacks and are unable to offer prompt and efficient ways of defence. One significant flaw in intrusion detection systems based on abuse detection is their inability to detect unknown network incursions like zeroday attacks (Bilge & Dumitra, 2012).

For three areas of IoT security, AI offers automation and intelligence capabilities. First, unsupervised learning can automatically learn from data without recognized tags. Unsupervised learning extends from depending on label data to employing unlabeled data, which can significantly reduce the consumption of manually labelled data and maintain its effectiveness in the scenario without empirical data. One common lack of prior knowledge is the failure to get sample labels. By identifying similarities between input data, unsupervised clustering techniques like K-Means can (Jain, 2010), for instance, partition the input data into distinct clusters without assigning labels. Second, ensemble learning can use the results of various classifiers to vote and change the model's learning focus, so gradually and automatically enhancing the model effect and avoiding repeated manual tasks. The deviation brought on by a single scene can be effectively reduced and the applicability to new scenarios is increased by the combination of models from several scenarios. Additionally, reinforcement learning can enhance advantages by gradually optimizing the model through the use of a reward/punishment mechanism and adjusting learning tactics in a dynamic

environment. To ensure that IoT security models adapt to changes in new environments, maintain validity, and strengthen the active exploration ability of the model, RL can learn new strategies while continuously inputting new data. This lays the groundwork for the realization of active immunity to IoT security.

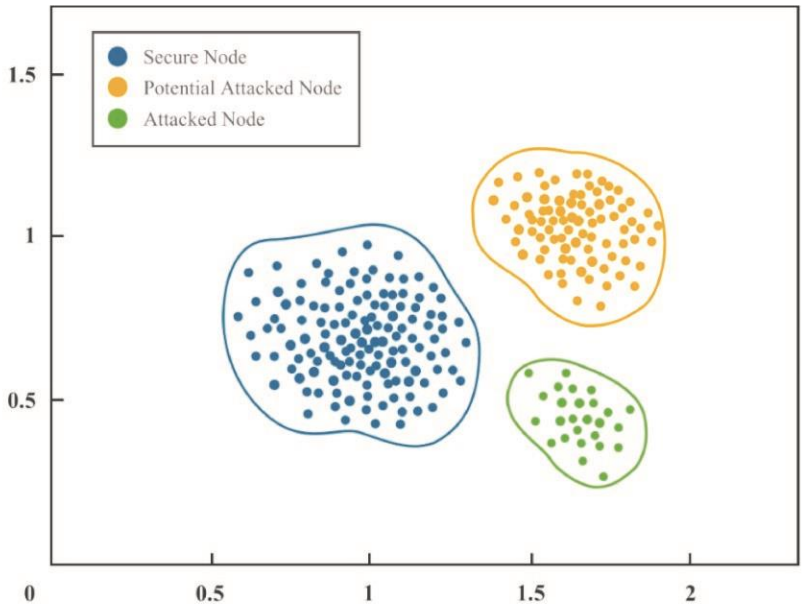

Figure 4. An example of IoT node clustering based on K-Means (Jain, 2010).

· **The ability to effectively process massive amounts of complex data:** Traditional IoT security protocols often function with a small amount of data. The shortcomings of these schemes in terms of big data processing capability and computing efficiency are highlighted by the increasing data generation. For instance, the main responsibility of software security in the application service layer is detecting malware. Traditional malware detection techniques extract malicious behavior codes from malware and store them as signatures. These techniques determine whether a new piece of software is malware by calculating how similar it is to the signature database. The computational complexity will increase quickly as the volume and dimensions of the data rise, which will substantially impair the model's efficiency and prevent it from making timely and accurate detections.

The advantage of AI methods over traditional methods is that they can not only analyze smallscale data but also use data sets with more samples and greater dimensions for efficient calculation.

One of the most well-known data sets in the area of image processing, for instance, is ImageNet (Deng et al., 2009). Its total data amount has surpassed 10 million, and several of its sub-datasets have over one million data. On some ImageNet subsets, numerous deep-learning models have nonetheless produced excellent results.

· **The ability to maintain great model accuracy:** IoT security urgently requires AI technology due to the low model accuracy of conventional models. The effectiveness of security models will be weakened if they are unable to predict a potential attack in time. Additionally, certain conventional models may harm the IoT's operating mechanism to enhance the model effect due to technical restrictions. For instance, the SYN Flood assault (Bogdanoski et al., 2013), a frequent DDoS attack, overloads the target server's connection queue by flooding it with a huge number of attack messages with faked source addresses. A defence mechanism is called Random Drop (RD). The queue pressure and server load can be reduced by RD by randomly deleting SYN requests from the TCP backlog queue. However, the success rate of many reliable clients with a regular connection or a sluggish connection will be significantly decreased, and some clients may even be unable to reply to SYN-ACK messages from the server, destroying TCP's operation mechanism altogether (Fujinoki, 2005). Large data sets can be calculated efficiently using AI techniques, and at the same time, these techniques can guarantee that models are effective and perform well across a variety of evaluation metrics, including precision and recall. In numerous application settings, supervised learning techniques and deep neural networks have produced excellent results.

· **The ability to provide model robustness and generalizability:** Problems are typically resolved by traditional security measures in settings that are uncomplicated settings. It's possible that these solutions won't deliver the desired outcomes when applied to more complicated situations, such as enterprise IoT security. For instance, conventional password device authentication is only appropriate for closed, limited systems since the password form's simplicity makes it simple to impersonate and capture passwords (Shimizu et al., 1998). AI techniques place a high value on robustness and generalization capabilities. Robustness calls for the model to be able to successfully minimize the effects of noise and outliers and ensure that the model can continue to function well in complicated settings (Bhagoji et al., 2018). The model's capacity to generalize shows its ability to predict outcomes for unidentified data, which assures that the model will maintain its efficacy when applied to situations other than the experimental setting (Neyshabur et al., 2017). Numerous machine learning techniques have advantages in terms of robustness and generalization capacity. For example, SVM determines the classification outcome using a small number of support vector samples; adding or deleting non-support vector samples has no impact on the model, which results in SVM having a good level of robustness. The random forest has good anti-noise ability and is insensitive to outliers. Linear models with L1 and L2 regularization have excellent generalization capacity and can prevent over-fitting (Moore & DeNero, 2011). The applicability and scalability of IoT security solutions can be considerably improved by using ML techniques with strong robustness and generalization capabilities.

4. IoT Security Threats

A. Four IoT Security Threats

According to the investigation, device authentication, DoS/DDoS attacks, intrusion detection, and malware detection are the four risks that need to be addressed immediately in IoT security. The traditional approaches to these issues have numerous flaws, including low efficiency and subpar realtime performance, and are unable to handle enormous data quantities. Most of them are not transferrable to IoT. Massive amounts of IoT data can be used by AI techniques included in machine learning to derive information from the data and anticipate future events, offering fresh approaches to these issues

i. Device Authentication

When information is exchanged, and data is transmitted between IoT nodes, there is a danger of interception, forgery, tampering, and destruction. The security needs between nodes include identity authentication, judgment, and blocking malicious nodes in order to avoid the transmission of fraudulent information (Zhang et al., 2015a). The authentication procedure for IoT devices tends to be limited by the IoT's characteristics, such as its resource limitations. To prevent the device from consuming excessive amounts of resources, it is vital to guarantee that the calculation and communication costs do not exceed the device's capabilities (Zhang et al., 2015b).

ii. DoS / DDoS Attack

Large-scale damaging attacks on the target system can be launched using denial-of-service (DoS) attacks (Chang, 2002), distributed denial-of-service (DDoS) attacks (Zargar et al., 2013), or vulnerabilities in servers and systems. Massive data packets that are larger than the intended processing capacity will overwhelm the network's bandwidth resources, causing program buffer overflow, hindering the normal requests of other recognized users, and finally triggering network service paralysis or system failure. Between DDoS and DoS, there are some differences. DDoS uses several distributed attackers in various positions to attack one or more targets simultaneously. Alternatively, an attacker may manage several machines in various locations and use those machines to attack the target.

iii. Intrusion Detection

The goal of intrusion detection is to keep track of system events by gathering and analyzing data on key points and looking for actions that go against security rules to accomplish early intrusion detection (Mukherjee et al., 1994). Intrusion detection, which offers real-time defence against internal and external threats, is a crucial component of network security as an active security protection solution. For the IoT network to quickly reestablish its network infrastructure, the capability to identify breaches or intrusions and malicious activity is essential.

iv. Malware Detection

IoT enables numerous smart devices to connect to one another in order to exchange information and enhance user experience (Moser et al., 2007). More and more PC or mobile applications are being developed to offer interactive services to users. One popular attack strategy is using the flaws in these applications to insert and run malicious malware in IoT software. These malware injection vulnerabilities might be connected to the application's authentication and authorization processes. Malicious code injection may also be made possible through physical interference with IoT devices, software alterations, and incorrect configuration of security settings. Bots, ransomware, adware, etc., are examples of common malware.

B. Overall Process of AI Solutions for IoT Security

Device authentication, DoS/DDoS attack detection, intrusion detection, and malware detection all fall under the category of classification tasks. For instance, AI-based solutions for device authentication must properly distinguish between approved and unauthorized devices; similarly, solutions for intrusion detection must distinguish between normal and abnormal network behaviours.

- **Collection of Data:** Most often, ML solutions need data sets from certain scenarios. You must select the proper setting for data collection for each problem to create training and test data sets. For instance, to account for user differences data sets for device authentication must include details about device setups, user behaviour, and patterns of use.
- **Pre-exploration and Pre-processing of Data:** The effectiveness of solutions is closely associated with the quality of training data. IoT data sets are generated by different sensors in different fields. The original data set does, however, include more or less issues, such as inconsistent data distribution and missing data. To prepare for the following steps, it is therefore important to mine the training data, master the data distribution, and then perform operations like eliminating errors and completing the data that is incomplete.
- **Model Selection:** For IoT security, there are numerous ML models to choose from, but each model has a set of scenarios in which it can be used. As such, we should choose the right models based on the traits of the models and the specifications of the problems. The selection of the model will also depend on the size of the data set and the outcomes of any preliminary investigation of the data. For instance, lightweight algorithms like Naive Bayes can produce expected results when the data set comprises fewer simple samples and training must be finished quickly.
- **Data Conversion:** The data acquired in real applications is typically inconsistent with the input data needed by models, therefore it must be translated to satisfy the requirements of the models we choose. For instance, it is important to do data conversion because the audio data gathered by voice sensors cannot be directly entered into RNN models. Extraction of the Mel-Frequency

Cepstral Coefficients (MFCC) from the original audio data is one of the conversion techniques (Hasan et al., 2004).

- **Training and Testing:** Data must be entered into models for training after model selection and data pre-processing are finished. To properly modify the learning rate or other parameters and ensure that the model effect is gradually maximized, we can observe the loss function value or result curve during the training process. Following the creation of training models, the generalization capability of the training models is tested using test datasets taken from the real world. Parameters must be changed again since training models may be under or overfitting (Jabbar & Khan, 2015).
- **Evaluation and Deployment of Models:** We can use a few effect indicators to compare various models after training before choosing the final one for actual deployment and application. Different evaluation metrics are used per issues like classification, regression, and ranking to impartially assess the model's propensity for prediction and generalization. Accuracy, precision, recall, F1 score (Rijsbergen, 1979), AUC (Area Under ROC Curve) (Bradley, 1997), and other metrics are frequently employed as evaluation indicators for IoT security.

A. DoS/DDoS Attack Detection and Defense Using AI

DoS and DDoS security relies on the filtration and cleansing of unusual traffic. Traditional DDoS and DoS defenses employ anti-DDoS technology, firewalls, or other security settings and are improved for load-balancing. Through firewall, rule, and content filtering, these approaches determine whether the external access traffic is normal. Due to the enormous number of devices and scarce resources in the IoT sector, IoT devices are becoming increasingly difficult to defend against DoS and DDoS attacks, necessitating effective and precise traffic filtering techniques. Intelligent and automated DoS/DDoS detection systems can be provided via machine learning.

I. Consumer IoT

Smart appliances and devices that can be worn are examples of consumer IoT that are vulnerable to DDoS attacks. Attacks are not similar to the IoT traffic of these devices. In order to detect attacks, ML can capture traffic that significantly deviates from the network traffic characteristics of particular behaviors of consumer IoT devices, such as DDoS activity. Doshi et. al (2018) use of a variety of ML methods, including K-nearest neighbors, decision trees, neural networks, random forests, and SVM, allowed for high-precision DDoS detection in consumer IoT traffic. The findings demonstrated that a home gateway router can automatically identify the source of a local IoT device's DDoS attack using traffic data and low-cost ML algorithms.

ii. Wireless Sensor Network

A DoS attack could target a wireless sensor network (WSN), an essential mode of communication in an IoT system. Deep learning has aided in the design of a secure media access control (MAC) protocol against WSN-oriented DoS attacks, which is now an active research direction. A novel secure MAC protocol based on Multilayer Perceptron (MLP) was proposed by Kulkarni et. al (2009). Each WSN node in this MAC protocol is running a trained MLP on the MAC layer. The collision rate, packet request rate, average packet waiting time, and other important environmental information are extracted by this novel MAC protocol and used as MLP's inputs. The likelihood (suspicion factor) of nodes being the target of a DoS attack will be outputted by MLP. The node will shut down and conserve energy if the suspicion factor exceeds the predetermined threshold, restricting the attack to a localized region of the network. Shutting down the attacked nodes decreases power consumption and extends the system's useful life.

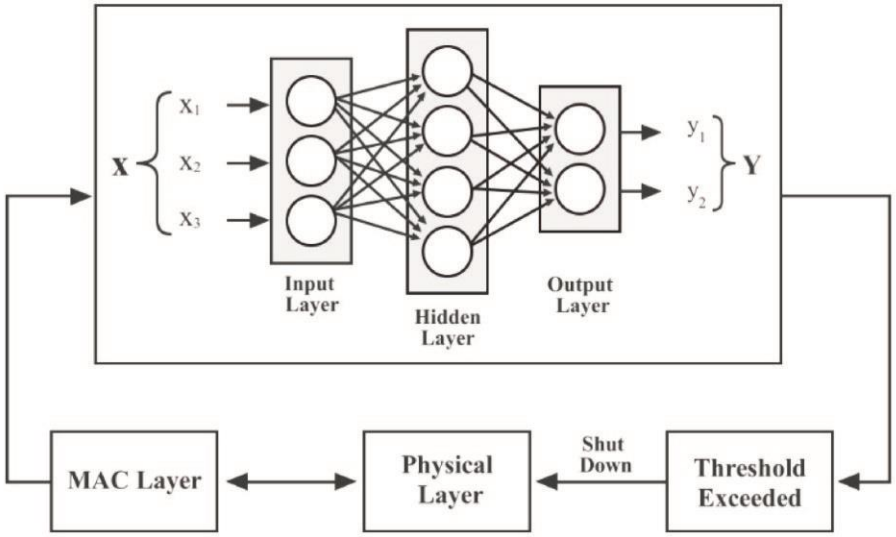

Figure 5. Secure MAC protocol combined with MLP by Kulkarni et. al (2009)

iii. Software-Defined Network

The control plane and data plane of network devices are separated in a network architecture known as a Software-Defined Network (SDN). Organizations can successfully manage IoT devices thanks to the SDN control plane's great functions. SDN can be employed as the IoT's foundational communication infrastructure because of its characteristics of centralized control, flexibility, and scalability. The SDN interfaces' openness, nevertheless, also has security repercussions and makes them susceptible to DDoS attacks. A DDoS detection method based on SVM that treated attack detection as a classification problem was put out by Ye et al. (2018). The method extracts information about DDoS attacks from the switch flow table of the SDN architecture, including the speed of the source IP, source port, and flow entries, the standard deviation of the flow packets, the deviation of the flow bytes, and the ratio of pair-flow, which are then used as characteristic values for SVM classification.

A. Intrusion Detection With AI

i. Traditional Intrusion Detection:

New intrusion types have created new issues for intrusion detection with the growth of the IoT. Although there is still an increase in intrusion through illegal access to gain sensitive information, solutions like access control, data encryption, and firewalls have some limits. Misuse detection or anomaly detection is a common technique used by intrusion detection systems today. Using attack patterns that have surfaced, misuse detection can efficiently identify known assaults (Yhung et al., 2000). They are unable to identify recent types of intrusions, for example zero-day attacks, because they differ from well-known attacks. Anomaly detection (Chandola et al., 2009), in contrast, examines typical traffic patterns and makes decisions based on the presumption that attackers behave differently from typical users. Traffic is seen as an intrusion if it differs significantly from common traffic patterns in terms of its characteristics. Anomaly detection is helpful for identifying new attacks, but it is less efficient than misuse detection for identifying established assaults. It takes a lot of time to find unusual behaviour in vast amounts of data. The process of anomaly detection still needs to be improved in terms of speed and precision.

When used for intrusion detection, machine learning has outperformed older methods. Intrusion detection has undergone new modifications as a result of machine learning (ML), which has also produced various new development trends, including the shift from single models to combined models, from emphasizing method correctness to considering method efficiency and effectiveness, and from centralized detection to decentralized detection.

ii. From Single Models to Combined Models:

Hybrid intrusion detection, which combines misuse detection and anomaly detection, has been proposed in certain research as a way to address the drawbacks of the two detection techniques listed above. The majority of hybrid detection systems independently train models for misuse and anomaly detection before combining their outputs. In contrast to conventional techniques, Kim et al. (2014) suggested a novel combination detection approach that hierarchically integrates a misuse detection model and an anomaly detection model (Figure. 6). In the integration phase, the ability to detect unknown assaults can be supplemented by the misuse model's ability to capture existing attacks. A C4.5 decision tree was first trained using training data made up of normal traffic and known attack traffic to create a model for misuse detection. Following this, 1-class SVMs were trained using training data for unknown attacks to create several anomaly detection models. The combined model outperformed a single traditional model in the test in identifying both known and unknown attacks.

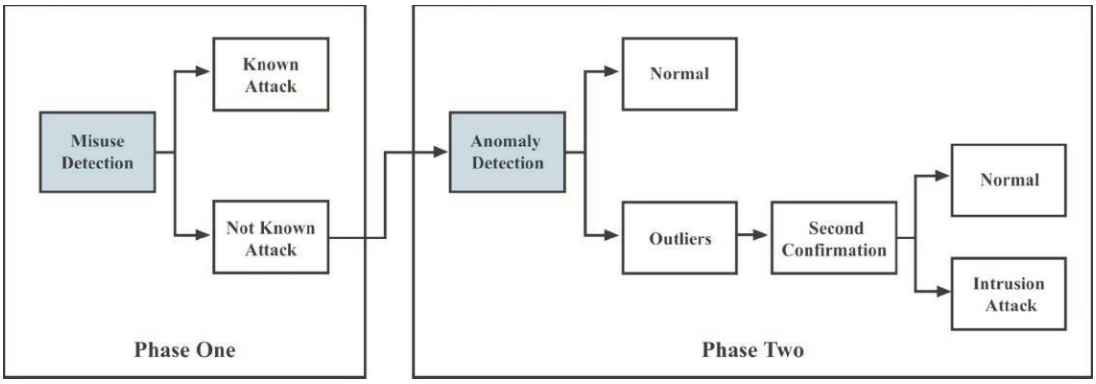

Figure 6. Combined intrusion detection by Kim et al. (2014)

I. Changing The Focus from Just Accuracy to Including Efficiency and Effectiveness In general, most intrusion detection systems place less emphasis on efficiency and more on effectiveness. It is crucial to select fewer but more significant features for intrusion detection systems since too many data features may not ensure optimal performance but instead lengthen decisionmaking processes. An approach to increase the effectiveness of intrusion detection is through the feature selection of ML.

To account for both efficiency and effectiveness, Li et al. (2019) designed a two-stage combined model. The Swarm Intelligence (SI) algorithm's heuristic iterative search capability was employed in the initial step to look for the best attributes. The second stage involved using random forest to classify the network traffic into several attack types using the features chosen in the first stage as inputs. The model enhanced its operation efficiency, opted for more significant features, and performed better at detecting intrusions. To increase the efficiency of intrusion detection, Su (2011) presented a feature selection approach combining KNN and GA. The fact that each data feature in a KNN is assigned the same weight although in reality some features may be ignored or have a higher priority than others is a significant drawback. Finding the ideal feature weight vector is the aim of GA in addition to KNN. A search algorithm called a genetic algorithm (GA) simulates the process of natural evolution to obtain the best answer. A population that reflects the problem's potential solution set serves as the foundation of GA. The "survival of the fittest" principle states that generations to come will generate better and better approximate solutions. The ideal weight vector for KNN can be found after GA evolution. The researchers extracted 35 features from network protocol header data, including IP, TCP, UDP, ICMP, ARP, and IGMP, to serve as initial training data. They then utilized the suggested algorithm to choose a few key features for intrusion detection. The overall accuracy for known attacks was 97.42% when the first 19 features were taken into account. Using the first 28 features correctly for unidentified attacks had a 78% success rate. Under the assumption that the effectiveness of detection would essentially be guaranteed, the approach significantly increased the time efficiency of intrusion detection.

The combined intrusion detection method discussed above can reduce computational complexity of models by decomposing the dataset in addition to feature selection methods that can increase efficiency (Kim et al., 2014). The training and testing time will be greatly decreased when the training dataset is broken down into smaller subsets, achieving the goal of enhancing time efficiency.

A. Device Authentication Using AI

i. Traditional Device Authentication:

There are numerous issues with traditional authentication technologies. For instance, even though password authentication is straightforward and easy to set up, it is typically only appropriate for closed systems. Every time a user logs into the system, they must input their password in plaintext, which puts their private information at risk of being revealed if the message is intercepted. Because identification information is static, traditional IoT terminals are easy to counterfeit (Li et al., 2019). The static nature of the device ID or user ID makes it simple for hackers to scan, read, and forge the identity. ML offers a variety of workable concepts for IoT secure authentication. These schemes employ a range of techniques to get valid information about devices and users.

Digital certificates are used to authenticate users and contain information about the user's identity. Users can access CA servers by using the authentication certificate, which relies on a reputable third-party Certification Authority (CA). The X.509 standard of the International Telecommunication Union specifies a framework for offering authentication services. Since general CA digital certificates adhere to the X. 509 standard, they are also known as X.509 certificates (Adams et al., 2001). In advance, the user's name and password are saved for password authentication (Shimizu et al., 1998). To ensure that a user's identity is valid, the system compares the information they submit with the information they have already saved.

ii. Human Behavior Characteristics

Manipulating objects habits, gaits, and handwriting are examples of human behavior characteristics that are frequently employed as identity authentication information. Smart security doors, smart air conditioners, smart refrigerators, smart TVs, and other indoor electronic devices can acquire human behaviour characteristics. Wi-Fi signals are strong between these devices. It is possible to capture the distinctive physiological and behavioural characteristics of human daily actions while using these devices (such as opening refrigerator doors, entering or leaving a room), offering a practical method for differentiating each person. Recognizing user activity must start with simple acts and progress to the distinctive behaviours of various users. The system must be equipped with abstract capabilities that may extract various granularities of feature representation. This is possible thanks to deep learning's strong abstract representation capabilities. To extract representative human

behaviour features from Wi-Fi signals from household appliances, Shi et al. (2017) integrated the amplitude and relative phase of the Channel State Information (CSI) with a three-hidden-layer DNN model (Figure. 7). This technique demonstrated the feasibility of combining Wi-Fi signals and DL by achieving authentication accuracy of 94% and 91% for dynamic and static human activity identification.

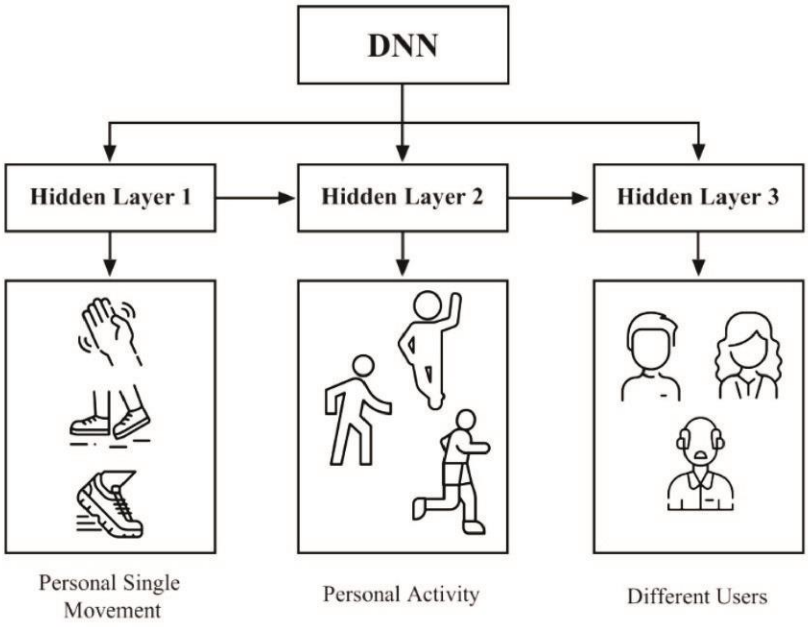

Figure 7: Shi et al. (2017) Abstract representation capability of DNN with three hidden layer

iii. Human Biological Characteristics

The term "human biological characteristics" refers to the physical traits that are unique to each person, such as their DNA, voices, faces, irises, and fingerprints. Identity verification can be done with the help of sound sensors included in wearable IoT devices like watches and smartphones. These gadgets frequently communicate with people in order to gather personal information, and they offer special advantages when it comes to precise user environment monitoring. For respiratory acoustics on mobile IoT devices, Breath Print is an authentication technology. Assuming that everyone has a distinctive breathing pattern, Breath Print uses the individual's respiratory acoustic features recorded by wearable IoT devices to provide user verification. Chauhan et al. (2018) used RNN with Breath Print to model the acquired respiratory acoustic data to distinguish distinct users, taking advantage of the special features of RNN in audio and speech processing. Studies have shown that this technique may be applied successfully with low latency (less than 200 ms for smartphones) on a variety of embedded devices with limited resources. Human biometrics are significant privacy data for users. Thus, it's critical to guard against potential privacy disclosure while using them. The original biometric data can be converted using the Cancellable Biometric System (CBS) technology. To prevent the original data from being destroyed, the converted data can at any time replace the original biological properties. With the

aid of image preprocessing, feature extraction, feature conversion, template matching, and other machine learning technologies, Punithavathi et. al (2019) developed a secure prototype of a light-weight cancelable biometric recognition system, solving the privacy issue associated with using human biological characteristics.

A. Malware Detection With AI

i. Traditional Solutions: Malware Detection Based on Signature

Malware behaviour libraries are created using signature-based malware detection, which provides distinctive signatures for each known malware (Venugopal & Hu, 2008). Experts find these signatures manually or automatically, and they can contain a variety of information, including file names, content strings, or bytes. To see if there are any matching signatures, one can compare the signature of unknown software with the malware behaviour library. This method, which has a quick detection rate and a low false alarm rate, is the most appropriate and popular detection method. However, just like the misuse intrusion detection, signature-based malware detection is ineffective against malware that has never been seen before. It's crucial to maintain and update the malware library regularly. But before any kind of detection or prevention can be carried out, there must be an initial victim who reports malicious activity. The consequences may be unacceptable when the initial victim is significant. For instance, the critical infrastructure flaws at the U.S. Office of Personnel Management in 2015 could trigger a series of events and chain reactions that last for decades (Scott, 2017).

ii. Networks Behaviours

To continuously gather information and manage the status of remote devices, the wireless multimedia system (WMS) is used. The majority of wireless multimedia devices come with several sensors that use routing tables to transfer data to nearby devices. The WMS's distributed topology facilitates malware's rapid spread, endangering other nodes, wireless routers, and terminals through data transmission. Identifying its network characteristics is essential for the detection of WMS malware. Using the data sniffer (DroidSniffer), in conjunction with SVM and BP neural networks to detect malware and stop harmful scripts, malware detection system made it easier to collect network behaviours in WMS (Zhou & Yu, 2018). The experiment's highest infection rate was only 22.17%, proving that malware can be found even when there are low infection rates.

iii. Graph and Opcode

When utilizing ML to identify malware, Opcode can be an acceptable and trustworthy feature. The combination of Windows malware opcodes with ML can identify malware efficiently thanks to the efforts and experiments of many researchers. The selected attributes (opcodes) of each sample (software) were transformed into a graph by Azmoodeh et al. (2019) (see Figure. 8). Nodes

represented the opcodes in their graph, and edges reflected each node's affinity (which must be calculated) in the disassembly file of each software. In order to employ CNN to categorize the generated graphs of harmful and benign software, graphs can be transformed into eigenspace (Chung, 1997). The opcode sequences of 1078 benign software and 128 malware programs were extracted for Azmoodeh's experiment. The detection accuracy of malware samples using graphs generated from opcodes was 99.68%, while the recall rate was 98.37%. Malware may be identified quite well using this technique.

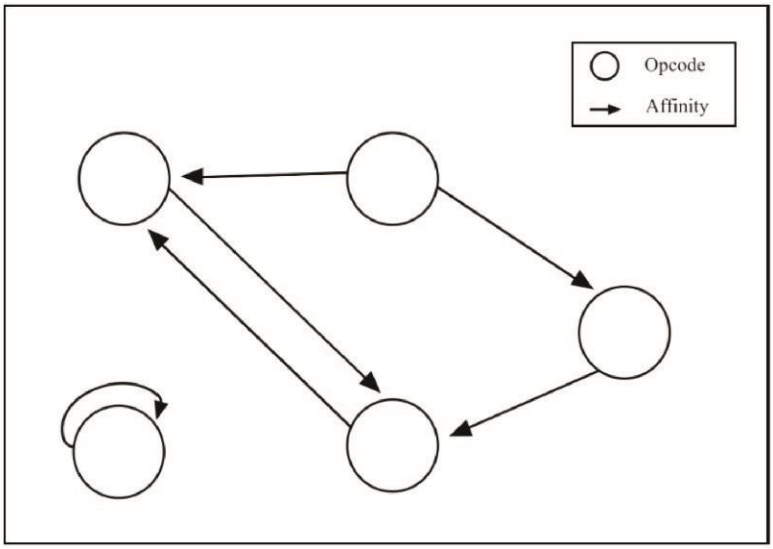

Figure 8. Azmoodeh et al. (2019).A graph converted from opcodes.

5. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

IoT security issues have been effectively addressed by artificial intelligence in several ways, but this does not imply that they have been fully resolved. In the areas of architecture, data and algorithms, and, there are still numerous difficulties to be resolved.

A. Architectural Challenges

The mobile and distributed IoT trends must be addressed when AI technologies are used in the IoT. The present IoT network and services heavily utilize the "Cloud-Channel-Device" architecture. To use the processing capacity of the vast computers in the data centre to calculate and make choices, the development of large-scale cloud computing centres may store and process a significant quantity of data in a centralized manner. The analysis findings are then returned to the device to create the interconnectivity effect. The C/S service architecture, which processes and responds to all requests and instructions through the central server, is also crucial for the transmission, storage, and processing of data.

The creation of supercomputing and storage capacities is made possible by the cloud service, which resolves issues with the high cost of building infrastructure and the underutilization of

computing and storage resources for small and medium-sized businesses. However, this is not appropriate in the IoT environment. The exponential growth in device connections and data generation presents the following difficulties for cloud architecture:

- When enormous amounts of data are transmitted to a cloud computing facility, the burden on the transmission bandwidth is drastically increased, causing a significant network delay that presents serious problems for scenarios where a delay is critical, such as autonomous vehicles, industrial manufacturing, etc.
- Data transmission uses a lot of energy, which places heavy pressure on cloud services.
- The exponential expansion of data produced by terminals cannot be matched by the linear growth of centralized cloud computing capabilities.

We are forced to execute data cleaning, processing, and decision-making at the source of the data due to the need for network transmission, data storage, and high-performance computing. The new edgebased architecture will play a significant role in the development of IoT architecture in the future. The original data application will be radically altered by distributed and edge architecture, which will impose more strict constraints on the use of AI in the field of IoT security.

B. Data Challenges

The use of AI techniques in the IoT space is based on data. Due to the heterogeneity of IoT, a lot of data is generated across several areas, which can cause a variety of issues, including poor data availability and quality, unforeseen hazards to data privacy, challenges with data integration, and more.

i. Data Sets' Availability

A lot of training data sets are needed for machine learning and deep learning. To achieve their great performance, the majority of deep learning techniques often rely on high-quality data (Zhang et al., 2018). The model's foundation for learning is a broad and varied set of training data. It is important to incorporate as much attack data that is representative of the actual world as possible because the quality of training data sets will have a direct impact on the model's performance. In addition to training data, the model also needs test data sets to evaluate and enhance training models by analyzing and comparing the generalization capacities of various algorithms.

ii. Data Cleaning

The process of eliminating duplicate information, fixing errors that have already occurred, and ensuring data consistency is known as data cleaning (Rahm & Do, 2000). According to estimates, anomalies and impurities make up roughly 5% of all data, which may be significantly higher for IoT. The following sorts of data must be cleaned:

- Incorrect Data. The business system is poor, which is the cause of the incorrect data. Without checking to see if the data is accurate when it is input, such as if the value is beyond its boundaries or the date format is incorrect, the data is written directly into the database. A database cannot be updated with inaccurate data until it has been examined and corrected, just like with incomplete data. Statistical analysis can reveal potentially incorrect or anomalous numbers; for instance, deviation analysis can reveal values that deviate from the distribution or regression equation. Incorrect data can also be detected using straightforward rules (common sense rules, business-specific rules, etc.) or restrictions between attributes.
- Incomplete Data. Data that lacks some information, like fields, is considered incomplete. Depending on the situation, incomplete data needs to be eliminated, supplemented, or abandoned. The database can only be updated with complete data. Missing values must often be filled in manually. The average, maximum, minimum, or more complex probability estimates can be used to replace some missing values that can also be determined from the data source.
- Duplicate Data. Duplicate records are those that have the same attribute value in the database.

To avoid compromising the use efficiency, it is required to combine similar records into a single record.

iii. Data Integration

IoT collects a ton of data via several sensor types, including RFID, ZigBee, and GPS, all of which must be properly integrated before they can be put to use. It might be difficult to integrate heterogeneous data while maintaining data quality since different data sources frequently contain heterogeneous data. Data integration is the process of logically or physically combining data from many sources, formats, and attributes to offer users full data sharing. Three categories can be used to group various forms of IoT data: There are three types of data: (a) structured data, like tables with rows and columns saved in traditional database systems; (b) semi-structured data, like HTML and XML files; and (c) unstructured data, like images and videos. In the area of enterprise data integration, a few frameworks are already available. Integrated systems are currently built using federal-based, middleware-based, and data warehousing techniques. These technologies address data integration and data exchange in various contexts and applications, offering businesses decision support. However, it is important to look into how these technologies apply to IoT data and make the necessary improvements.

iv. Data Privacy and Security

Processing and using data present issues in terms of data security and privacy. You run the risk of having your privacy compromised during the collection of data and transmission procedure. The system does not offer a trustworthy service level agreement (SLA) about the theft or misuse of users' personal information, which causes many users to doubt their security even if data encryption

enhances privacy protection (Marjani, 2017). For instance, the privacy of users might readily be threatened by personal information found in wearable device data. For medical diagnosis and service suggestions, wearable device data on the human body is used by personalized medical and healthcare applications. These individually identifiable data are quite detailed and frequently include location, identity, and physiological traits. Individual tendencies, behaviors, and preferences are simple to deduce. All parties involved in data collecting, management, and utilization in specific contexts, such as medical care, must exercise extreme caution in protecting personal information (Bertino, 2017). Medical diagnostic and service recommendations are made by healthcare applications using wearable device data collected from the human body. These individually identifiable data are quite detailed and frequently include location, identity, and physiological traits.

C. Algorithm Difficulties

Not only is artificial intelligence not perfect, but it also has several flaws. IoT inherits flaws from the use of ML to address security issues, requiring attention and improvement.

i. Poor Portability

Machine learning models are specific to a given field. The original model parameters may not work when a successful model for one scene is applied to additional challenges of a similar nature. To replace the existing model, new ones must be trained. The variety of IoT applications will require a wide range of models, all of which must be kept up to date. However, the retraining process is timeconsuming, and there will undoubtedly be several errors, which will consume a significant amount of computational power.

ii. Uncertainty

Little input changes may have different consequences on the output in ML and DL (Kapla Et Al., 2019). The output of models may change drastically even when the input data is altered. Attackers have the power to purposefully alter some input data, which leads to unstable systems and unexpected outcomes. Since the IoT environment generates an IoT of high-frequency data, it is crucial to maintain the integrity and stability of the input data. However, this is a difficult task.

iii. Resource Consumption and Computational Complexity

In contrast to IoT devices, ML and DL have computational complexity (Huang et al., 2019) and resource requirements. IoT devices are resource-constrained, and there are very few opportunities to acquire memory and computational resources. It will nevertheless take days or even weeks to complete the training even if numerous computational resources are allocated to some models linked to image, audio, and natural language processing. Consequently, it is important to design ML and DL frameworks that can efficiently minimize computational complexity in order to offer

effective security procedures. Future research should focus on minimizing computational complexity and resource consumption, particularly for large-scale IoT systems.

iv. Risks to ML/DL Security

Similar to IoT itself, the AI techniques employed to maintain IoT security carry varying degrees of security threats. The attacker may attempt to harm AI by poisoning it or by using evasion, impersonation, or reverse attacks (Liu, 2018). In order to make the model learn incorrect and invalid knowledge from the training data, poisoning, evasion, and impersonation attacks alter the training data by creating incorrect label samples, maliciously altering samples, and simulating samples. This reduces the classifier's ability to distinguish between normal and abnormal behaviors, which results in the failure of the detection function of models. Reverse attacks gather some basic data about the target model using the application program interface (API) offered by the current ML systems and then reverse analyze that basic data to utilize the target model to get private data, such as patient medical data. There will be major repercussions if these attack techniques are integrated with other IoT services.

D. Future Directions

Some of the aforementioned issues, such as the lack of data availability and the requirement for data integration, are intrinsic to the Internet of Things (IoT). Some of the new issues that AI presents for IoT include resource usage and the security of algorithms. We must develop new technology or enhance existing ones to combat these unseen threats. In addition to addressing these issues, we also suggest two potential new avenues in this paper.

i. Integrating Edge AI Chips in IoT Devices

The majority of traditional AI computing operations are currently carried out remotely on centralized core devices or platforms, but this isn't the greatest option for IoT. AI computations can now be integrated into IoT devices thanks to edge AI processors. Machine learning tasks can be carried out or expedited on edge devices using an edge AI processor (Zhou, 2019). The development of edge AI chip technologies, such as Google Coral Edge TPU is currently being accelerated by Google, NVIDIA, Intel, Qualcomm, and Huawei (Sengupta et al., 2020). Network conditions in many industrial domains are poor, and updating communication infrastructure is quite expensive. The use of edge AI chips allows terminals to conduct AI computations locally, significantly lowering transmission costs. Delays can be significantly reduced using edge AI chips. Because judgments must be made in real-time on numerous devices, edge computing has real-time demands. Real-time performance cannot be achieved with cloud computing or data center computing due to network latency.

Edge AI chips can also ensure the security and privacy of data. The computations don't have to send the original data back to the cloud, considerably enhancing data security and privacy while lowering the risk of data leakage, interception, or misuse of private or corporate information.

ii. Creating IoT Security Architectures that are Service-Oriented and Capable of Meeting the Requirements of Various Services in Various Fields.

IoT security must accommodate the unique security requirements of various application scenarios. It is a pressing issue to figure out how to develop flexible security architectures that can offer industrial applications adaptive and differentiated security assurance capabilities. The network infrastructure's capacity to enable Security-as-a-Service's open capability is crucial (Hafeez et al., 2015; Bhattasali& Chaki, 2016).

Network designs must establish security resources, such as authentication protocols, cryptographic algorithms, data encryption and decryption, etc., that are independent of devices and applications based on computing resources. We may construct security functions including trustworthy authentication, digital identity, operation maintenance, and management based on security resources. Then, utilizing these security features, we should construct platforms to offer security services to external applications via open APIs. Finally, a third party can flexibly employ the security capabilities and services supplied by the open platform to accomplish tailored security protection in the face of various IoT businesses with various security requirements. This architecture design can provide total security protection in comparison to third-party self-designed security solutions, and it can incorporate workable AI models in open platforms, considerably enhancing the third party's security potential. The security of IoT can also get a high elastic security capability thanks to the design's robust scalability.

6. Conclusion

In conclusion, this survey delved into the captivating realm of harnessing Artificial Intelligence (AI) to fortify the security landscape of the Internet of Things (IoT). With a comprehensive analysis of the existing literature, we embarked on a journey that underscored the pressing need for innovative solutions to the escalating security concerns within the IoT ecosystem. Our objective was to shed light on the manifold ways in which AI can be harnessed to bolster the security measures surrounding IoT devices and systems.

In essence, this review acts as a basis for future research projects that aim to explore the hidden opportunities associated with the interaction between AI and IoT security. It is crucial to keep a forward-looking view that foresees both obstacles and opportunities as AI models get more complex and the IoT ecosystem develops. We may strive towards an interconnected future where AI fortifies IoT security, ushering us into an era when innovation and protection coexist together, by fostering a continuous cycle of study, development, and deployment.

The research presented in this paper article shows that AI is useful for IoT security, especially for the four main threats of DoS/DDoS assault defense, intrusion detection, device authentication, and malware detection. Using the broad framework of the AI schemes that we have suggested, future IoT security challenges can be overcome. When employing AI for IoT security, any problems with data, algorithms, and architecture also need to be fixed in order to avoid the creation of new threats.

How to solve these issues may be the subject of future research.

References

Adams, C., Sylvester, P., Zolotarev, M., &Zuccherato, R. (2001). Internet X.509 public key infrastructure data validation and certification server protocols. Request Comments, 3029, 15.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A., Du, X., Ali, I., &Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Commun. Surveys Tuts. Advance online publication. https://doi.org/10.1109/COMST.2020.2988293

Al-Sarawi, S., Anbar, M., Alieyan, K., & Alzubaidi, M. (2017). Internet of Things (IoT) communication protocols: Review. In Proc. 8th Int. Conf. Inf. Technol. (ICIT) (pp. 685–690).

Azmoodeh, A., Dehghantanha, A., & Choo, K. K. R. (2019). Robust malware detection for Internet of (Battlefield) Things devices using deep eigenspace learning. IEEE Trans. Sustain. Comput., 4(1), 88-95. https://doi.org/10.1109/TSUSC.2018.2809665

Bauer, M., Boussard, M., Bui, N., Loof, J. D., Magerkurth, C., Meissner, S., Nettsträter, A., Stefa, J., Thoma, M., & Walewski, J. W. (2013). IoT reference architecture. In Enabling Things to Talk (pp. 163-211). https://doi.org/10.1007/978-3-642-40403-0_8

Bertino, E. (2016). Data security and privacy in the IoT. In Proc. EDBT (pp. 1-3).

Bezawada, B., Bachani, M., Peterson, J., Shirazi, H., Ray, I., & Ray, I. (2018). Behavioral fingerprinting of IoT devices. In *Proceedings of the Workshop on Attacks Solutions Hardw. Secur.* (pp. 41-50).

Bosman, H. H. W. J., Iacca, G., Tejada, A., Wörtche, H. J., & Liotta, A. (2015). Ensembles of incremental learners to detect anomalies in ad hoc sensor networks. *Ad Hoc Networks*, 35, 14-36. https://doi.org/10.1016/j.adhoc.2015.07.013

Bhagoji, N., Cullina, D., Sitawarin, C., & Mittal, P. (2018). Enhancing robustness of machine learning systems via data transformations. In Proc. 52nd Annu. Conf. Inf. Sci. Syst. (CISS) (pp. 1–5).

Bhattasali, T., & Chaki, N. (2016). Poster: Exploring security as a service for IoT enabled remote application framework. In Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services Companion (pp. 15).

Bilge, L., & Dumitra, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. In Proc. Comput. Commun. Secur. (pp. 833–844). https://doi.org/10.1145/2382196.2382284

Bisht, P., & Venkatakrishnan, V. N. (2008). XSS-GUARD: Precise dynamic prevention of cross-site scripting attacks. In Proc. Int. Conf. Detection (pp. 23–43). https://doi.org/10.1007/978-3-54070542-0_2

Bogdanoski, M., Shuminoski, T., & Risteski, A. (2013). Analysis of the SYN flood DoS attack. Int. J.

Comput. Netw. Inf. Secur., 5, 1–11.

Bradley, A. P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. Pattern Recognition., 30(7), 1145–1159. https://doi.org/10.1016/S00313203(96)00142-2

Castelvecchi, D. (2016). Can we open the black box of AI? Nature, 538(7623), 20-23. https://doi.org/10.1038/538020A

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1-58. https://doi.org/10.1145/1541880.1541882

Chang, R. K. C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. IEEE Commun. Mag., 40(10), 42–51. https://doi.org/10.1109/MCOM.2002.1039856

Chauhan, J., Seneviratne, S., Hu, Y., Misra, A., Seneviratne, A., & Lee, Y. (2018). Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks. *Computer*, 51(5), 60-67. https://doi.org/10.1109/MC.2018.2381119

Chettri, R., Pradhan, S., & Chettri, L. (2015). Internet of Things: Comparative study on classification algorithms (k-NN, naive Bayes and Case based Reasoning). Int. J. Comput. Appl., 130(12), 7–9. https://doi.org/10.5120/IJCA2015907120

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J. C. (2004). Client-side defense against Webbased identity theft. In Proc. Netw. Distrib. Syst. Secur. Symp. (p. 15). Retrieved from http://simson.net/ref/2005/csci_e-170/ref/webspoof.pdf

Chuankun, W., Zhang, L., &Jiangli, L. I. (2017). Design of trust architecture and lightweight authentication scheme for IoT devices. NetinfoSecur., 17(9), 16–20.

Chung, F. R. (1997). Spectral Graph Theory (No. 92). American Mathematical Society.

Chen, L., Ye, Y., &Bourlai, T. (2017). Adversarial machine learning in malware detection: Arms race between evasion attack and defense. In Proc. Eur. Intell. Secur. Inform. Conf. (pp. 99-106).

Chung, C. Y., Gertz, M., & Levitt, K. (2000). DEMIDS: A misuse detection system for database systems. In *Proceedings of the Working Conference on Integrity and Internal Control in Information Systems* (pp. 159-178). https://doi.org/10.1007/978-0-387-35501-6_12

Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity, and availability in security. J. Inf. Syst. Secure., 10(3), 21-45. Retrieved from http://www.proso.com/dl/Samonas.pdf

Diro, A. A., &Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761-768.

Demontis, A., Melis, M., Biggio, B., Maiorca, D., Arp, D., Rieck, K., Corona, I., Giacinto, G., & Roli, F. (2019). Yes, machine learning can be more secure! A case study on Android malware detection. IEEE Trans. Dependable Secure Comput., 16(4), 711-724.

Deng, J., Dong, W., Socher, R., Li, L.-J., Li, K., & Fei-Fei, L. (2009). ImageNet: A large-scale hierarchical image database. In Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (pp. 248–255).

Deogirikandar, A., &Vidhate, A. (2017). Security attacks in IoT: A survey. In Proc. Int. Conf. (pp. 32-37).

Dorai, R., & Kannan, V. (2011). SQL injection-database attack revolution and prevention. J. Int. Commer. Law Technol., 6(4), 224–231. https://doi.org/10.4028/www.scientific.net/AMM.740.810

Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. In Proc. IEEE Secur. Privacy Workshops (SPW) (pp. 29–35). https://doi.org/10.1109/SPW.2018.00013

Elisseeff, A., & Weston, J. (2002). A kernel method for multi-labelled classification. In Proc. Adv. Neural Inf. Process. Syst. (pp. 681–687).

ETSI. (2019). Cyber Security for Consumer Internet of Things (document TS103645).

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). Android security: A survey of issues, malware penetration, and defenses. IEEE Commun. Surveys Tuts., 17(2), 998–1022. https://doi.org/10.1109/COMST.2014.2386139

Fujinoki. (2005). Cached Guaranteed-Timer Random-Drop against TCP SYN-flood Attacks and Flash Crowds. In Proc. IASTED Int. Conf. Commun., Netw., Inf. Secur. (Vol. 2005, pp. 162–169).

Elisseeff, A., & Weston, J. (2002). A kernel method for multi-labelled classification. In Proc. Adv. Neural Inf. Process. Syst. (pp. 681–687).

Gislason, D. (2008). Zigbee Wireless Networking (pp. 3–14). Oxford, U.K.: Newnes.

Hafeez, I., Ding, A. Y., Suomalainen, L., Hätönen, S., Niemi, V., &Tarkoma, S. (2015). Cloud-based security as a service for smart IoT environments. In Proc. 2015 Workshop Wireless Students (p. 20).

Hai-ming, C. (2010). Key technologies and applications of Internet of Things. Comput. Sci., 36(6), 1–4.

Hasan, M. R., Jamil, M., & Rahman, M. (2004). Speaker identification using mel frequency cepstral coefficients. Variation, 1(4), 25.

Huang, H., Song, Y., Yang, J., Gui, G., & Adachi, F. (2019). Deep-Learning-Based millimeter-wave massive MIMO for hybrid precoding. IEEE Trans. Veh. Technol., 68(3), 3027-3032. https://doi.org/10.1109/TVT.2019.2893928

ITU Internet Reports (2005): *The Internet of Things*, Geneva, Switzerland. International Telecommunication Union, 2005.

Jabbar, S., & Khan, R. Z. (2015). Methods to avoid over-fitting and under-fitting in supervised machine learning (comparative study). In Proc. Comput. Sci., Commun. Instrum. Devices (pp. 163–172).

Jain, A. K. (2010). Data clustering: 50 years beyond k-means. Pattern Recognit. Lett., 31(8), 651–666. https://doi.org/10.1016/j.patrec.2009.09.011

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Netw., 20(8), 2481–2501. https://doi.org/10.1007/S11276-014-0761-7

Kaplan, A., Nordman, D. J., & Vardeman, S. B. (2019). On the S-instability and degeneracy of discrete deep learning models. Inf. Inference, 12, 1-29. https://doi.org/10.1093/imaiai/iaz022

Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690-1700. https://doi.org/10.1016/j.eswa.2013.08.066

Kolias, C., Kambourakis, G., Stavrou, A., &Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80-84. https://doi.org/10.1109/MC.2017.201

Kulkarni, R. V., &Venayagamoorthy, G. K. (2009). Neural network-based secure media access control protocol for wireless sensor networks. In *Proceedings of the International Joint Conference on Neural Networks* (pp. 3437-3444). https://doi.org/10.1109/IJCNN.2009.5179075

Li, J., Zhao, Z., Li, R., &Zhang, H. (2019). AI-based two-stage intrusion detection for software-defined IoT networks. *IEEE Internet of Things Journal*, 6(2), 2093-2102. https://doi.org/10.1109/JIOT.2019.289304

Lenzerini, M. (2002). Data integration: A theoretical perspective. In Proc. Symp. Princ. Database Syst. (pp. 233-246). https://doi.org/10.1145/543613.543644

Li, Z., Zuoyue, W., Chundong, W., Yunfei, M. A., &Chaocan, X. (2019). Design and implementation of intelligent identification system for IoT terminals. *Journal of Chongqing University Posts Telecommunications*, 31(4), 443-450.

Liang, G. (2015). Automatic traffic accident detection based on the Internet of Things and support vector machine. Int. J. Smart Home, 9(4), 97–106. https://doi.org/10.14257/ijsh.2015.9.4.10

Liaw, A., & Wiener, M. (2007). Classification and Regression by Random Forest. Retrieved from http://cogns.northwestern.edu/cbmg/LiawAndWiener2002.pdf

Lin, Y., Zhu, X., Zheng, Z., Dou, Z., & Zhou, R. (2019). The individual identification method of wireless device based on dimensionality reduction and machine learning. *Journal of Supercomputing*, 75(6), 3010-3027. https://doi.org/10.1007/s11227-018-2487-2

Liu, Q., Li, P., Zhao, W., Cai, W., Yu, S., & Leung, V. C. M. (2018). A survey on security threats and defensive techniques of machine learning: A data driven view. IEEE Access, 6, 12103-12117. https://doi.org/10.1109/ACCESS.2018.2805680

Lo, S.-C. B., Chan, H.-P., Lin, J.-S., Li, H., Freedman, M. T., & Mun, S. K. (1995). Artificial convolution neural network for medical image pattern recognition. Neural Netw., 8(7–8), 1201–1214. https://doi.org/10.1016/0893-6080(95)00061-5

Madaan, A., Wang, X., Hall, W., &Tiropanis, T. (2018). Observing data in IoT worlds: What and how to observe? In Proc. Living Internet Things, Cybersecurity (IoT) (pp. 1–7). https://doi.org/10.1049/cp.2018.0032

Mahdavinejad, M. S., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P., & Sheth, A. P. (2018). Machine learning for Internet of Things data analysis: A survey. Digit. Commun. Netw., 4(3), 161–175. https://doi.org/10.1016/J.DCAN.2017.10.002

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. IEEE Access, 5, 5247-5261. https://doi.org/10.1109/ACCESS.2017.2689040

Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., &Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. arXiv:1709.04647. Retrieved from http://arxiv.org/abs/1709.04647

Moore, R., & DeNero, J. (2011). L1 and L2 regularization for multiclass hinge loss models. In Proc. Symp. Mach. Learn. Speech Lang. Process. (p. 15).

Moser, A., Kruegel, C., &Kirda, E. (2007). Exploring multiple execution paths for malware analysis. In Proc. IEEE Symp. Secur. Privacy (pp. 231–245). https://doi.org/10.1109/SP.2007.17

Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. IEEE Netw., 8(3), 26–41. https://doi.org/10.1109/65.283931

Murphy, K. P. (2006). Naive Bayes Classifiers. Vancouver, BC, Canada: University of British Columbia.

Neyshabur, B., Bhojanapalli, S., McAllester, D., & Srebro, N. (2017). Exploring generalization in deep learning. In Proc. Adv. Neural Inf. Process. Syst. (pp. 5947–5956).

Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M., & Choo, K.-K.-R. (2019). A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences*, 484, 255-268. https://doi.org/10.1016/j.ins.2019.02.066

Rahm, E., & Do, H. H. (2000). Data cleaning: Problems and current approaches. Eng. Bull., 23, 3-13. Retrieved from http://dc-pubs.dbs.unileipzig.de/files/Rahm2000Data/Cleaning/Problemsand.pdf

Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., & Bouabdallah, A. (2013). A systemic approach for IoT security. In Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst. (pp. 351–355).

Rijsbergen, C. (1979). Information Retrieval. Newton, MA, USA: Butterworth-Heinemann.

Ringnér, M. (2008). What is principal component analysis? Nature Biotechnol., 26(3), 303–304. https://doi.org/10.1038/nbt0308-303

Safavian, S. R., & Landgrebe, D. (1991). A survey of decision tree classifier methodology. IEEE Trans. Syst., Man, Cybern., 21(3), 660–674. doi: 10.1109/21.97458.

Schuster, M., & Paliwal, K. K. (1997). Bidirectional recurrent neural networks. IEEE Trans. Signal Process., 45(11), 2673–2681. https://doi.org/10.1109/78.650093

Scott, J. (2017). Signature based malware detection is dead. Washington, DC, USA: Institute for Critical Infrastructure Technology. Retrieved from https://icitech.org/wpcontent/uploads/2017/02/ICIT-Analysis-Signature-Based-Malware-Detection-is-Dead.pdf

Sengupta, J., Kubendran, R., Neftci, E., & Andreou, A. (2020). High-speed, real-time, spike-based object tracking and path prediction on Google edge TPU. In Proc. 2nd IEEE Int. Conf. Artif. Intell. Circuits Syst. (AICAS) (pp. 134-135).

Singla, A., Mudgerikar, A., Papapanagiotou, I., &Yavuz, A. A. (2015). HAA: hardware-accelerated authentication for Internet of Things in mission-critical vehicular networks. In Proc. MILCOM - IEEE Mil. Commun. Conf. (pp. 1298-1304). https://doi.org/10.1109/MILCOM.2015.7357624

Sinha, R. S., Wei, Y., & Hwang, S.-H. (2017). A survey on LPWA technology: LoRa and NB-IoT. ICT Exp., 3(1), 14–21. https://doi.org/10.1016/J.ICTE.2017.03.004

Shi, C., Liu, J., Liu, H., & Chen, Y. (2017). Smart User authentication through actuation of daily activities leveraging WIFI-enabled IoT. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing* (pp. 1-7). https://doi.org/10.1145/3084041.3084061

Shimizu, A., Horioka, T., & Inagaki, H. (1998). A Password Authentication Method for Contents Communications on the Internet. IEICE Trans. Commun., 81(8), 1666–1673.

Su, M.-Y. (2011). Real-time anomaly detection systems for Denial-of-Service attacks by weighted knearest-neighbor classifiers. *Expert Systems with Applications*, 38(4), 3492-3498. https://doi.org/10.1016/j.eswa.2010.08.137

Su, J., Vasconcellos, V. D., Prasad, S., Daniele, S., Feng, Y., & Sakurai, K. (2018). Lightweight classification of IoT malware based on image recognition. Comput. Softw. Appl. Conf., 2, 664669. https://doi.org/10.1109/COMPSAC.2018.10315

Venugopal, D., & Hu, G. (2008). Efficient signature-based malware detection on mobile devices. *Mobile Information Systems*, 4(1), 33-49.

Watkins, C. J. C. H., & Dayan, P. (1992). Q-learning. Mach. Learn., 8(3–4), 279–292.

Wu, C., Shi, J., Yang, Y., & Li, W. (2018). Enhancing machine learning based malware detection model by reinforcement learning. In Proc. 8th Int. Conf. Commun. Netw. Secur. (pp. 74-78).

Yerima, S. Y., Muttik, I., & Sezer, S. (2015). High accuracy Android malware detection using ensemble learning. *IET Information Security*, 9(6), 313-320. https://doi.org/10.1049/ietifs.2014.0099

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Comput. Netw., 52(12), 2292-2330. https://doi.org/10.1016/J.COMNET.2008.04.002

Zargar, S. T., Joshi, J., &Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun. Surveys Tuts., 15(4), 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127

Zhang, Q., Yang, L. T., Chen, Z., & Li, P. (2018). A survey on deep learning for big data. Inf. Fusion, 42, 146-157. https://doi.org/10.1016/J.INFFUS.2017.10.006

Zhang, Y. T., Yan, C. H., & Wei, Y. R. (2015). Research on security of IoT perception layer based on node authentication. Netinf. Secur., 15(11), 27–32.

Zhong, C. L., Zhu, Z., & Huang, R. G. (2015). Study on the IOT architecture and gateway technology. In Proc. 14th Int. Symp. Distrib. Comput. Appl. Bus. Eng. Sci. (DCABES) (pp. 196–199). https://doi.org/10.1109/DCABES.2015.56

Zhou, W., &Yu, B. (2018). A cloud-assisted malware detection and suppression framework for wireless multimedia system in IoT based on dynamic differential game. *China Communications*, 15(2), 209-223. https://doi.org/10.1109/CC.2018.8300282

Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2019). Edge intelligence: Paving the last mile of artificial intelligence with edge computing. Proc. IEEE, 107(8), 1738-1762.

Zhu, D., Jin, H., Yang, Y., Wu, D., & Chen, W. (2017). Deep Flow: Deep learning-based malware detection by mining Android application for abnormal usage of sensitive data. In Proc. IEEE Symp. Comput. Commun. (ISCC) (pp. 438-443).