ANALYTICAL STUDY ON ENABLING ARTIFICIAL INTELLIGENCE FOR SECURITY IN IOT

Dr. Satish Kumar Gupta
HOD & Associate Professor IT, Rajan Mamta Degree College, Aurangabad Bihar,
ait.satish@gmail.com

Dr. Atul Agrawal
Associate Professor, Sushila Devi College of Technology, Indore (MP)
atul.273@gmail.com

Govind Kumar
Research scholar, Faculty of Information Technology, Gopal Narayan Singh University, Sasaram
Bihar, govindcuh@gmail.com

Dibya Prakash
Assistant Professor, Rajan Mamta Degree College, Aurangabad Bihar
dibyaprakash18102000@gmail.com

Abstract

In most fields, maximizing efficiency and reducing costs are of paramount importance. Because most aspects of the 4th industrial revolution (4IR) are technological in nature, the performance and cost matrices may vary between industries, but cybersecurity will always be essential. The Internet of Things (IoT) has various security issues, similar to those of other Internet-based technologies, namely in the areas of access control and exposed services. The use of AI to improve security is a potential new direction. With the use of IoT, businesses can easily collect real-time data on all of their operations' physical components. The role of artificial intelligence (AI) is growing in IoT applications and businesses, signaling a change in strategy for companies operating in this space. Companies around the world are rapidly adopting IoT technology to develop cutting-edge products and services, paving the way for novel market niches and strategic directions. As a result, businesses will have to adapt to a new era in terms of how they conduct their operations and interact with their clientele. An enormous opportunity awaits businesses that can transform raw IoT data into actionable business intelligence, and the key to doing so lies in robust information diagnostics.

Keywords: IOT, Artificial intelligence, Technology, Security

INTRODUCTION

The Internet of Things (IoT) is the development and expansion of existing online infrastructure and services. Physical items and their interconnections in the modern world are described. In order to connect or exchange data over the internet, IoT employs the Application Programming Interface (API), sensors, mobile phones, and actuators. Everything can talk to everything else that's linked to the internet. Automatic identification and inter-object communication are also expected to become commonplace. The power of the Internet of Things has far-reaching effects on people's routines and habits. Primarily, it is implemented in cutting-edge computer, networking, and communication systems, as well as embedded devices, sensor networks, and internet protocols. The IoT's network of connected devices is rapidly being put to use to gather information, disseminate that information, and take appropriate actions on their own. Those gadgets capture and share information over the internet because to the electronics, software, and sensors inherent inside them. These nodes are often self-configuring and intended for savvy communication with nearby nodes. Solutions for data transport, access, and usage have been proposed by data communication developers and cyber security engineers.

LITERATURE

Kah Phooi Seng et.al (2022) The Internet of Things as we know it today is the product of progress in and the coming together of sensor, information processing, and communication technologies. A new set of difficulties has emerged for the Internet of Things due to the exponential growth in needed data and services. To create the artificial intelligence Internet of Things, innovative technologies and smart methodologies may be decisive in fostering the growth of intelligent structures and services in the IoT. A survey of recent developments in AI for IoT is presented here, as well as a discussion of the various computational frameworks being developed in this area, as well as a discussion of the opportunities and obstacles facing the effective deployment of this technology to solve complex problems in a wide range of applications. This article surveys the present landscape of study at the interface of AI and the Internet of Things (IoT), with a particular emphasis on four main areas: AI IoT architectures, methodologies, and hardware platforms. Sensors, devices, energy strategies, and the Internet of Things (IoT communication)'s and networking infrastructure, as well as its applications, all based on artificial intelligence. The article goes on to talk about how artificial intelligence Internet of Things may be made possible via the use of smart sensors, edge computing, and software-defined networks.

Anshul Jain et.al (2021) The fundamental objective of this research was to develop an AI-enabled, low-cost security solution for an Internet-of-Things (IoT)-enabled healthcare environment. Healthcare services are easier to establish, more effective, and have more features added because to this. The purpose of this research is to use artificial neural networks to construct a methodology for making predictions about potentially malicious devices based on their data transfer rates. COVID has mandated that all outlying areas must have access to healthcare over the internet. However, healthcare ecosystem services need dependable, high-speed infrastructure that also safeguards the privacy of patient information. This paper's method solves the problems of both security and service disruption. In this study, we present a neural network-based approach to identify and deactivate malicious hardware without disrupting essential services. In our prior work, we used a manual approach to detecting intrusions based on our own expertise; this study is an improvement on that method. All of the tests performed for this study were related to the healthcare industry. There are six distinct slices that correspond to the device mobility pattern. All clients connected to slices were routinely watched by the security module, and any devices deemed troublesome or suspicious were removed using machine learning. To automatically identify and stop potentially harmful gadgets, we have trained a neural network in MATLAB and deployed it to analyze the dataset. Accurate values with unique characteristics have been sought via the use of a variety of network designs and training methods in MATLAB. Five training cycles were carried out and compared, yielding an optimal R=99971. We set up the program to work with the four most common scenarios. To evaluate and verify our forecasts, we also simulated an experimental application. In this research, we provide a method to ensure the safety of an IoT-based healthcare network. An end-to-end solution on the segmented network is implied by the proposed architectures. Artificial neural networks are used effectively to identify and disable potentially harmful hardware. In addition, the solution is adaptable, configurable, and deployable in a wide variety of ecosystems, including those concerned with home automation.

Nagaraja Seshadri et.al (2020) In this paper, we explore how the IoT (Internet of Things) is fostering the emergence of a fully digital world in which each and every object is interconnected, thereby fostering the development of ever-greater levels of intelligence and the optimization of previously inefficient procedures. Internet of Things (IoT) challenges are discussed alongside its architecture, technologies, components, and applications. When digital and physical components are combined, as they are in the IoT, productivity is boosted, time spent on tasks is reduced, higher quality products are produced, and significant opportunities for new invention are unlocked. This paper provides a concise summary of the design process for a smart home automation architecture that allows users to remotely access and manage a wide range of home appliances from a mobile application. A variety of high-tech parts are used to create the home automation program. Each component of the system, which includes numerous home appliances, is preprogrammed, remote controlled, and meticulously monitored. In this paper, we will also go over the security requirements for the Internet of Things (IoT) and the major challenges and security risks associated with the IoT.

Ashwini.S et.al (2019) The number of people who use the internet grows larger every day, and it's possible that by next year there will be billions and billions of them. More and more people are using their smartphones to sync up their various appliances with the web, which helps them save time and provides for more accurate data transmission. The internet serves as a platform for many different types of content, including those pertaining to communication, entertainment, medicine, health, daily life, and education, all with the goal of expanding the market. The proliferation of Android devices may lead to a corresponding increase in the vulnerability of our cloud-stored personal information. Most IoT-connected devices and their capacity for making decisions regarding sensitive matters, such as real-world sensor data or malware, are the focus of this research. Methodologies used in the business world to keep sensitive information safe; methods for finding malware, etc. This research has aroused our curiosity in learning more about Resilient management in IoT devices following malware detection, and we aim to do so in the near future.

Spyros G Tzafestas (2018) The Internet of Things (IoT) is a relatively new technological breakthrough that has been widely and positively accepted in many fields of today's information society. In particular, the success of a wide variety of day-to-day applications is greatly boosted by the inclusion of IoT devices and systems that are backed by artificial intelligence. Our goal with this essay is to present a broad overview of the most pressing concerns related to the integration of IoT and AI, including both existing and future applications that might have significant societal impact. The article begins with a brief introduction to the Internet of Things (IoT) and artificial intelligence (AI), and then goes on to define "IoT-AI synergy," provide examples of "IoT facilitated by AI," and briefly discuss "Industrial IoT," "Internet of Robotic Things," and "Industrial Automation IoT." (IAIoT). Several examples are then provided, followed by a discussion of how the Internet of Things and artificial intelligence may be used to improve robotics and factory automation.

ARTIFICIAL INTELLIGENCE AND ITS IMPORTANCE

Artificial intelligence (AI) refers to the capabilities of a high-powered computer or PC-detailed robot to carry out activities normally associated with sentient beings. Artificial intelligence (AI) refers to computer devices that can replace human knowledge in the demonstration of intentional actions. Because of mimicked knowledge, robots can easily learn new information, adapt to new sources, and do tasks that were previously reserved for humans. Since its inception, mimicked knowledge has been integrated into the workforce, and this trend is only expected to grow as its many advantages become more widely known and accepted. Figure 1: Examples of AI's many uses.

Figure 1. Artificial Intelligence Applications

INTERNET OF THINGS AND ITS IMPORTANCE

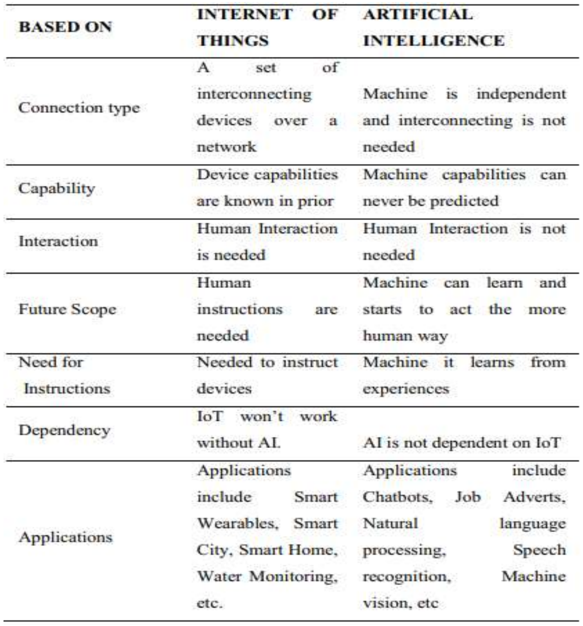
The term "Internet of Things" (IoT) is used to define the interconnected system of physical things that may collect and transmit data via the Internet without the intervention of human operators. These methods range from the simple (but outdated) literature on the nuclear family to the sophisticated (and cutting-edge) tools of today.

With the help of IoT, devices and objects can monitor, identify, and understand a situation or environmental conditions independently of human intervention. Everything from everyday items like kitchen appliances, cars, indoor regulators, and kid screens to the internet through implanted devices is connected. In the same way that AI knowledge is widely employed in various officialdooms, so too is IoT knowledge. Implementations of the Internet of Things are shown in Figure 2.

Figure 2. IoT Applications

- Manufacturing — When sensors report an approaching hardware breakdown, proactive support may be activated with the help of creation line checking.
- Automotive — Currently cruising automobiles may show a pattern of discontent with their equipment, as detected by sensors, alerting the chauffeur with subtleties and suggestions.
- Retail - Control inventory, expand product and service knowledge, facilitate a more adaptable supply chain, and lower operational costs.
- IoT asset-monitoring applications will lag behind in the healthcare industry.

Table 1. Table of differences between the IoT and AI



BASED ON	INTERNET OF THINGS	ARTIFICIAL INTELLIGENCE
Connection type	A set of interconnecting devices over a network	Machine is independent and interconnecting is not needed
Capability	Device capabilities are known in prior	Machine capabilities can never be predicted
Interaction	Human Interaction is needed	Human Interaction is not needed
Future Scope	Human instructions are needed	Machine can learn and starts to act the more human way
Need for Instructions	Needed to instruct devices	Machine it learns from experiences
Dependency	IoT won't work without AI.	AI is not dependent on IoT
Applications	Applications include Smart Wearables, Smart City, Smart Home, Water Monitoring, etc.	Applications include Chatbots, Job Adverts, Natural language processing, Speech recognition, Machine vision, etc

The use of artificial intelligence is desirable in every sector. Artificial intelligence is being used in:

- For the purpose of providing individualized medical care, including prescription adjustments, X-ray interpretations, and other personalized medical services.
- It is the goal of this service to (1) allow customers to make purchases online using provider-modified recommendations and (2) have a say in the purchasing decisions made on their behalf.
- Using discontinuous frameworks to analyze real-time production line data for estimates of load and demand.
- The Board of Directors is attempting to learn how to recognize potentially fraudulent trades, master rapid and accurate credit scoring, and automate truly uncommon data in order to: The emotional biases of humans aren't necessary for artificial intelligence to make rational decisions. Because AI never tires or gets weary, it never needs to take a break, relax, or get involved.

IOT SECURITY CHALLENGES

There are new concerns about device and data security as a result of the widespread adoption of IoT technology in the manufacturing sector. There are a growing number of connected devices, as evidenced by various global statistics. As a result of this growth, more security threats and difficulties may emerge. There may be restrictions on implementing IoT systems because of security concerns. The authors speculate that this trend could make sound security practices even more important in the Internet of Things sector.

Improved participation of cybersecurity professionals in the Internet of Things is a goal of several initiatives developed by NIST. Standards, guidelines, and tools for securing Internet of Things (IoT) products, connected devices, and their deployment environment are being encouraged by this initiative.

- Threats to Data Integrity and Availability The following are some of the most frequently encountered security threats to IoT systems:
  - The complexity of identifying and comprehending security requirements increases due to the interconnectedness of IoT's many moving parts and the wide range of technologies it employs.

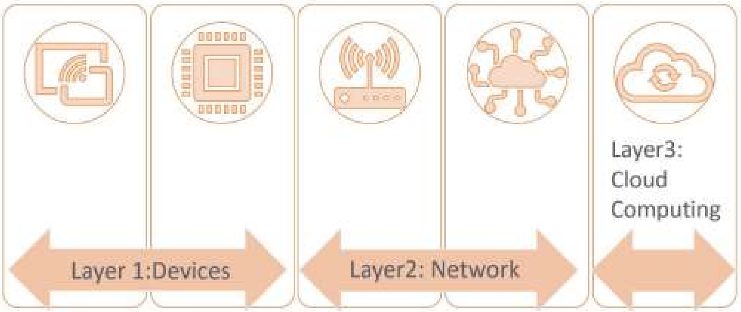


Figure 3. IoT architecture.

◦ Devices in an Internet of Things network typically have limited capabilities. Because of this, these gadgets have become the weakest point in cyber defenses.

◦ There are potential security risks associated with the incorporation of mobile devices into the IoT because of the need for them to be flexible.

◦ Also known as "Big data," the data produced by the Internet of Things is enormous. The latter presents its own challenges in terms of administration and safety.

◦ Because of the wide variety of IoT applications, there may be equally diverse security needs. Industry-specific use cases and supporting infrastructure for Internet of Things deployments, may necessitate a rethinking of the needs and, by extension, the security measures put in place. Table 3 provides a summary of the most frequently encountered IoT security requirements.

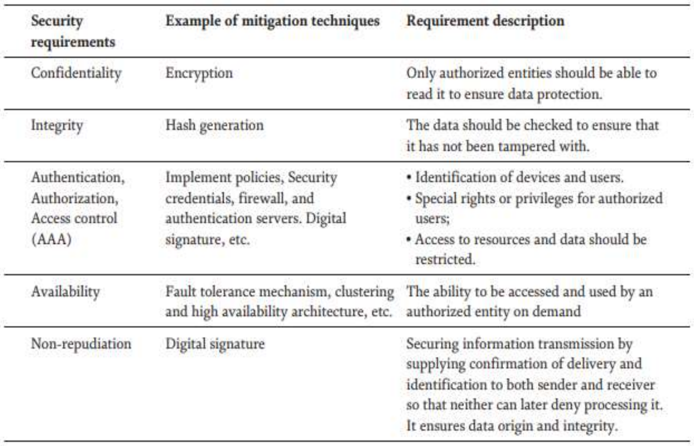
Inadequacies in the capacity and competence of IoT devices to implement traditional security solutions need new approaches, it is extremely difficult to meet all of the aforementioned requirements.

Artificial intelligence categories

Several philosophical groundworks have been done in the area of artificial intelligence (AI). Russell distinguishes between "weak" AI, in which a machine can perform intelligent actions, and "strong" AI, in which a machine can actually think. However, the implementation of AI system features is improved when hybrid mechanisms are used.

There are two main types of AI, distinguished by the mechanisms they employ to achieve intelligence via data processing. The

Table 2. IoT security attributes, techniques and requirements



Security requirements	Example of mitigation techniques	Requirement description
Confidentiality	Encryption	Only authorized entities should be able to read it to ensure data protection.
Integrity	Hash generation	The data should be checked to ensure that it has not been tampered with.
Authentication, Authorization, Access control (AAA)	Implement policies, Security credentials, firewall, and authentication servers. Digital signature, etc.	• Identification of devices and users. • Special rights or privileges for authorized users; • Access to resources and data should be restricted.
Availability	Fault tolerance mechanism, clustering and high availability architecture, etc.	The ability to be accessed and used by an authorized entity on demand
Non-repudiation	Digital signature	Securing information transmission by supplying confirmation of delivery and identification to both sender and receiver so that neither can later deny processing it. It ensures data origin and integrity.

The first type is the expert system, which is knowledge-based and whose central feature is the presence of an inference engine.

ARTIFICIAL INTELLIGENCE IN INDUSTRIAL IOT

The significance of AI in IIOT

Industrial Internet of Things (IIoT) devices provide a wealth of data available, making artificial intelligence (AI) adoption a breeze. Knowledge inference and analytics assistance are both aided by AI techniques. The most pressing issues that need to be studied are threat hunting and intelligence, blockchain technology, edge computing, and the protection of users' personal data, with potential solutions proposed.

Given the significance and sensitivity of the information being shared, the volume of data created by IIoT is large, and real-time computation is a major cause of this. Artificial intelligence may help meet this need for big data analysis while maintaining a low latency. Finding out what a company does is essential when designing security and privacy solutions. This is a difficult operation even in a conventional industrial system, and IIoT adds much more sophistication to the mix. There are several approaches to implementing AI technology, including computing paradigm and security, however interoperability issues are seen as a significant barrier to adoption.

Over time, the Internet of Things (IoT) has evolved from a theoretical idea employed by academics and IT firms to a practical reality. Certain businesses and government agencies have fully integrated IoT into their daily operations. New uses for the Internet of Things (IoT) are cropping up in every sector of society. Applications of IoT technology in the real world are shown in Figure 2 and include smart homes, smart health, intelligent transportation, smart cities, smart agriculture, and industrial automation.

In fact, Factories are first on the list of the top five sectors where the Internet of Things adds the most economic value, according to the same McKinsey & Company report described above, moving on to human health, work sites, cities, and retail environments. The analysis suggests that by 2030, the Internet of Things may bring in between $5.5 trillion and $12.6 trillion, with the majority of that growth coming from business-to-business uses of the technology.

THE IOT BUSINESS MODEL

The term "business model" refers to an organization's method of value creation, distribution, and capture. Whether for better or worse, a company's business relationships and model will be impacted by its adoption of Internet of Things technologies. The most popular organizational structures will be covered here.

A pioneering effort to create a business model for the Internet of Things was released in 2015. The studies aimed to determine which components are necessary for

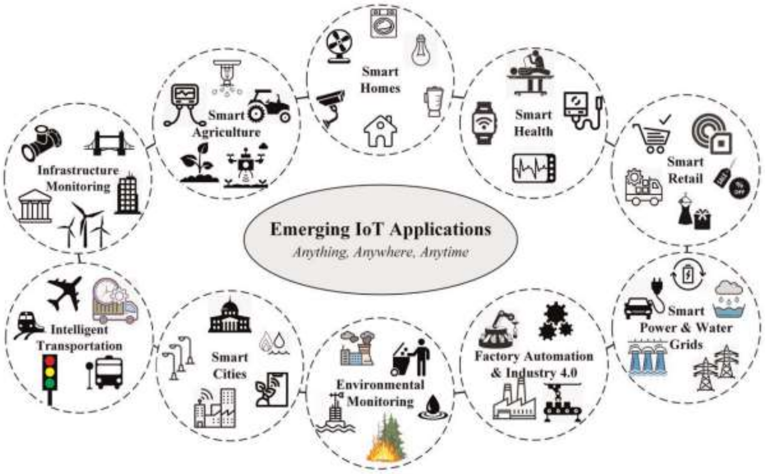

Smart Homes
Smart Agriculture
Smart Health
Infrastructure Monitoring
Smart Retail
Emerging IoT Applications
Anything, Anywhere, Anytime
Intelligent Transportation
Smart Power & Water Grids
Smart Cities
Environmental Monitoring
Factory Automation & Industry 4.0

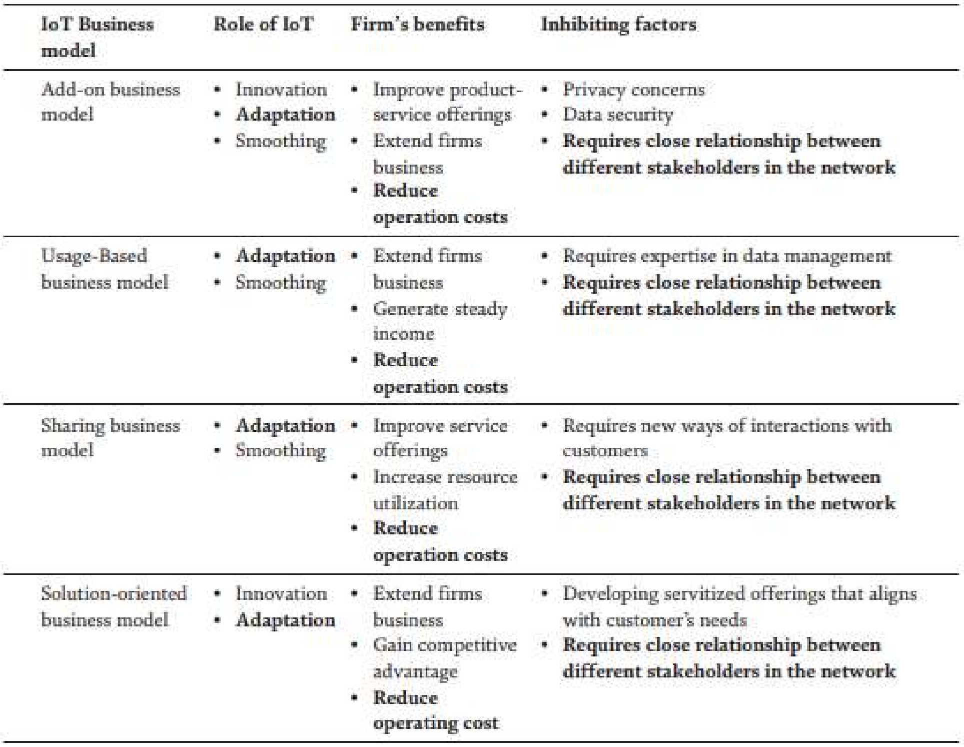
Figure 4. Use of IoT technology

IoT enterprise models, including the various components available and their relative significance. In this model, the value proposition was found to be the most critical component of IoT business models. Next in line in terms of significance were "customer relationships" and "key partnerships." The AIC model, presented in, is another conceptual IoT Business Model that emphasizes implementation of IoT in specific contexts. Aspiration, Implementation, and Contribution are the three stages that make up this model. At this first stage, called "Aspiration," you will define and foresee the value that will be generated by implementing IoT. A company should look into how the Internet of Things can help their business by gaining a competitive edge or by developing superior products and services during the strategy development phase of the Implementation process. The third phase, called Contribution, requires an organization that has decided to adopt IoT to investigate the viability of the strategy, as well as the skills and means at its disposal for putting it into action. In other words, does the company have the expertise required to successfully implement IoT?

There are four categories that servitized business models that utilize the Internet of Things fall into. We looked at the role of IoT in each business model, the benefits to the company, and any potential roadblocks. IoT business models are presented and compared across the aforementioned three lenses in Table 4, which is adapted from the original study. It is important to note the similarities between the four distinct business models, such as the fact that adaptation is a key function for the Internet of Things, that lowering operating costs is a widespread advantage, and that a key barrier to adoption is the necessity of close relationships among various stakeholders.

Different types of Internets of Things deployment call for unique business models. As a result, there isn't a single model that can be applied to all industries. The study's authors analyzed seven different IoT business models. Their research led them to identify six features of the Internet of Things business model:

Table 3. Classifying business models by their functions, advantages, and drawbacks



IoT Business model	**Role of IoT**	**Firm's benefits**	**Inhibiting factors**
Add-on business model	• Innovation • **Adaptation** • Smoothing	• Improve product-service offerings • Extend firms business • **Reduce operation costs**	• Privacy concerns • Data security • **Requires close relationship between different stakeholders in the network**
Usage-Based business model	• **Adaptation** • Smoothing	• Extend firms business • Generate steady income • **Reduce operation costs**	• Requires expertise in data management • **Requires close relationship between different stakeholders in the network**
Sharing business model	• **Adaptation** • Smoothing	• Improve service offerings • Increase resource utilization • **Reduce operation costs**	• Requires new ways of interactions with customers • **Requires close relationship between different stakeholders in the network**
Solution-oriented business model	• Innovation • **Adaptation**	• Extend firms business • Gain competitive advantage • **Reduce operating cost**	• Developing servitized offerings that aligns with customer's needs • **Requires close relationship between different stakeholders in the network**

- The capacity to detect the evolution of various business models.
- The opportunity to link Internet of Things elements with those of the business model.
- Being able to see how network-centric strategies relate to business-centric ones.
- Value Flow Mapping is the process of depicting how money is made, spent, and used in a company.
- Ability to strike a balance between taking action and broadening one's rational perspective; Possibility of incorporating digital business model patterns; Balance between taking action and expanding one's rational perspective.

CONCLUSION

In this Paper, we learned that businesses have been using Internet of Things (IoT) technology to create new industrial applications that offer tangible benefits to both the company and the customer, particularly in terms of efficiency and cost savings. We also examine a variety of business models to better appreciate why it's so challenging to create an industry-wide standard for the Internet of Things: businesses. Therefore, it is essential for businesses to take measures to protect the privacy of their customers' information and the integrity of their data. Due to the complexity of the IoT system, however, privacy and security have become issues in IIOT. The use of IoT and AI makes the commercial unthinkable and helps make it more impressive. Similarly, if these two developments converged, it would challenge risk-takers to achieve much more fundamental mechanized transformation. The benefits of bringing together these two developments can be reaped in vast quantities. It's not easy to merge AI and IoT in the entertainment industry, as doing so requires not only advanced theory but also new skills and authority. However, when taken as a whole, these inventive developments greatly affect businesses' ability to expand their profit margins.

REFERENCE

1. Nagaraja Seshadri et.al “Internet of things (IoT) and Security” International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Volume 8, Issue 15

2. Ashwini.S et.al “Design of Low Power Artificial Intelligence Model for Resilience of IoT Devices” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-3S, October 2019

3. Kah Phooi Seng et.al “Artificial intelligence Internet of Things: A new paradigm of distributed sensor networks” International Journal of Distributed Sensor Networks 2022, Vol. 18(3)

4. Anshul Jain et.al “Security as a Solution: An Intrusion Detection System Using a Neural Network for IoT Enabled Healthcare Ecosystem” https://doi.org/10.28945/4838

5. Spyros G Tzafestas “ynergy of IoT and AI in Modern Society: The Robotics and Automation Case” Case Report Volume 3 Issue 5 - September 2018
DOI: 10.19080/RAEJ.2018.03.555621

6. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications, pages 230–234. IEEE, 2014.

7. Wei Zhou, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. IEEE Internet of Things Journal, 6(2):1606–1616, 2018.

8. Yajin Zhou and Xuxian Jiang. Dissecting android malware: Characterization and evolution. In 2012 IEEE symposium on security and privacy, pages 95– 109. IEEE, 2012.

9. Zhi-Jie Zhou, Guan-Yu Hu, Chang-Hua Hu, Cheng-Lin Wen, and Lei-Lei Chang. A survey of belief rule-base expert system. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019.

10. Liang Xiao, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? IEEE Signal Processing Magazine, 35(5):41– 49, 2018.

11. Iqbal H Sarker, Alan Colman, Jun Han, Asif Irshad Khan, Yoosef B Abushark, and Khaled Salah. Behavdt: a behavioral decision tree learning to build user-centric context-aware predictive model. Mobile Networks and Applications, 25(3):1151–1161, 2020.

12. Ahmed Saeed, Ali Ahmadinia, Abbas Javed, and Hadi Larijani. Intelligent intrusion detection in low-power iots. ACM Transactions on Internet Technology (TOIT), 16(4):1–25, 2016.

13. Alice Corp. Pty. Ltd. v. CLS Bank International, 573 U.S. ___, 134 S. Ct. 2347, June 19, 2014. As of October 11, 2017: https://www.supremecourt.gov/opinions/13pdf/13-298_7lh8.pdf

14. Angwin, Julia L., Jeff Larson, Surya Mattu, and Lauren Kirchner, “Machine Bias: There’s Software Used Across the Country to Predict Future Criminals. And It’s Biased Against Blacks,” ProPublica, 2016. As of December 7, 2016.
15. Autor, David H., David Dorn, Lawrence F. Katz, Christina Patterson, and John Van Reenen, “Concentrating on the Fall of the Labor Share,” American Economic Review, Papers and Proceedings, Vol. 107, No. 5, pp. 180–185, May 2017a.
16. Satish Kumar Gupta(June - 2021) "Analytical Study on Training of Data set Generation and Construction in Machine learning using Genetic Algorithms" in Journal of Huazhong University of Science and Technology volume 50 PAPER ID: HST-0621-629.
17. Satish Kumar Gupta(April-2019) A Study of Machine Learning Using Genetic Algorithm, Journal of Emerging Technologies &Innovative Research ISSN UGC Approved (Journal No: 63975) & 7.95 Impact Factor Published in Volume 6 Issue 4 , ISSN:2349-5162
18. Satish Kumar Gupta (2018)“A Study on Training of Data Set Generation in Machine learning”, International Journal of Advance Research and Innovative Ideas in EducationVolume-4 Issue-1 201, Paper Id: 15215 and ISSN (O): 2395-4396.