Vol. 3 No. 2 (2025)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and Future Directions

Israr Ahmad[1]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
israr.gdec@gmail.com

Fawad Nasim[2]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
fawad.nasim@superior.edu.pk

Syed Khawar Hussain Shah[3]
Department of Computer Engineering, Bahria University, Islamabad, Pakistan. skhawar.h11@bahria.edu.pk

Muhammad Furqan Khawaja[4]
Bahria University Lahore Campus. furqankhawaja1@gmail.com

Syed Asad Ali Naqvi[5]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
syedasad.alinaqvi@superior.edu.pk

Hamayun Khan[6]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Abstract

The influence of AI in our society is becoming important due to the possibility of carrying out analysis of the large amount of data that the increasing number of interconnected devices capture and send as well as making autonomous and instant decisions from the information that machines are now able to extract, saving time and efforts in some determined tasks, specially in the cyberspace. The Internet of Things (IoT) is a technology with exponential growth in different applications such as transportation, healthcare, and manufacturing. It is expected to add 20 billion IoT devices globally by the end of 2025. IoT devices are important in monitoring machines' conditions and improving operational processes. However, these devices also have a vast surface of cyberattacks due to insufficient authentication methods, vulnerabilities in their firmware, and the lack of standardization. Integrating Artificial Intelligence (AI) in IoT systems further enhances their operational capabilities and potential benefits. Various Artificial Intelligence (AI) techniques have been adopted to optimize the efficiency of IoT applications, leading to a new computing paradigm, like Generative AI. The capability of Generative Artificial Intelligence to generate content and to autonomously learn and predict situations can be beneficial for making decisions automatically significantly enhancing the security of IoT systems. In this review article we provide an overview of Generative Artificial Intelligence-based existing solutions for the very diverse set of security issues in IoT environments and to try to anticipate future research.

Keywords: Artificial Intelligence, Cybersecurity, Internet of Things, Cyberattack, IoT Security

Introduction

The Internet of Things (IoT) is one of the leading technologies these days. The IoT applications appeared in different domains such as healthcare, transportation, manufacturing, and smart cities.

It includes many smart devices connected to a wide internet network using different network technologies that collect, exchange, and analyze data to improve the efficiency of decision-making processes [1, 2]. The use of Artificial Intelligence (AI) helps to understand, learn, reason and interact, increasing efficiency. AI technology such as Machine Learning allows extracting knowledge from large amounts of structured and unstructured data [3].

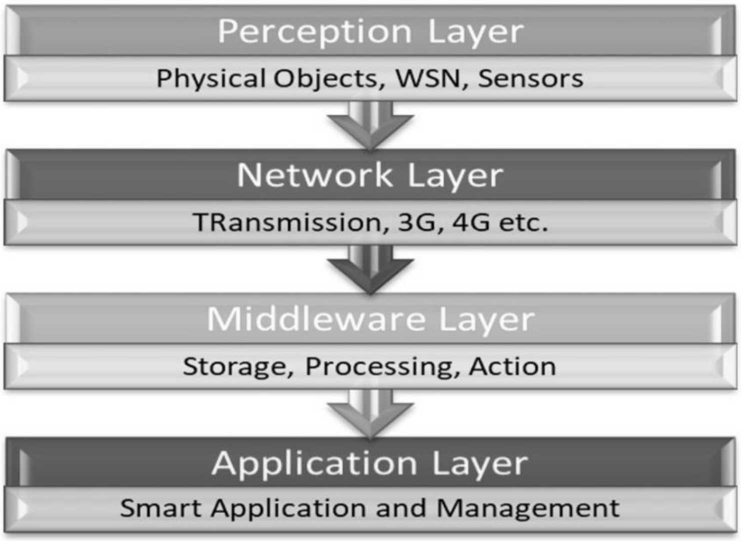

Perception Layer
Physical Objects, WSN, Sensors
Network Layer
TRansmission, 3G, 4G etc.
Middleware Layer
Storage, Processing, Action
Application Layer
Smart Application and Management

Figure 1: IoT Architecture [4]

According to [5] the total number of IoT connections including all IoT types reached 15.7 billion and it is estimated to become 38.8 billion by 2029. The rapid growth of IoT devices has also exposed the significance of vulnerabilities, making IoT systems an easy target for cybercriminals. A typical IoT application consists of four layers, the perception layer, network layer, middleware layer, and application layer.

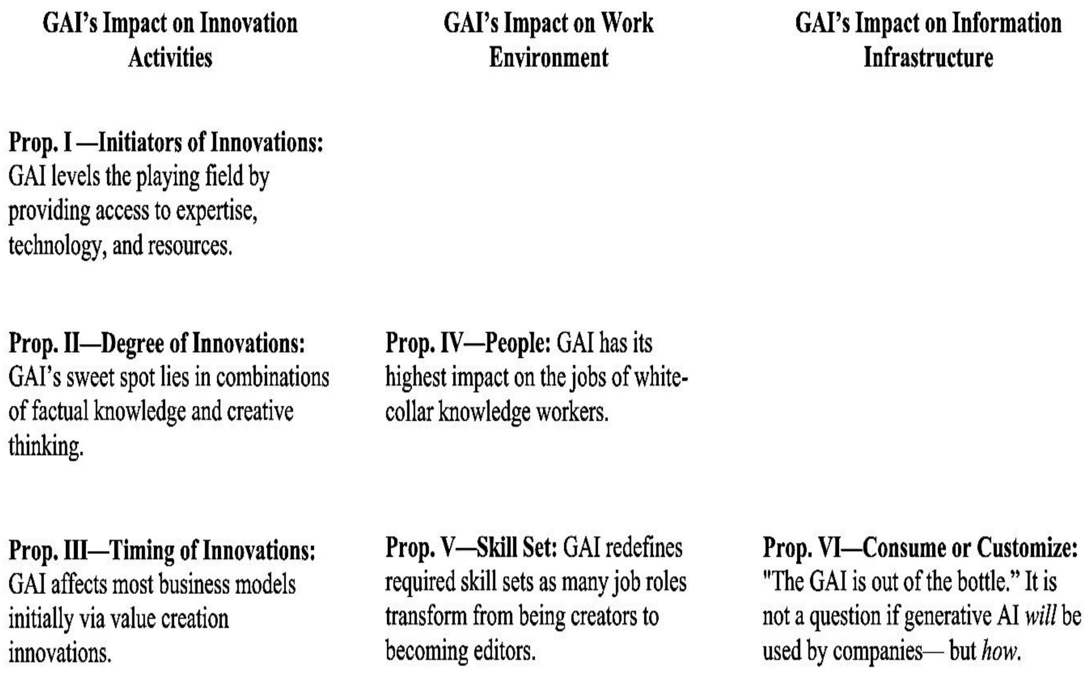
Perception Layer: In the perception layer, sensors and actuators are used to gather useful information like temperature, moisture content, intruder detection, sounds, etc., and send it to the network layer.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Network Layer: It gets data from the perception layer and passes to the middleware layer using network technologies like 3G, 4G, Wifi, Infrared, etc.

Middleware Layer: It has some advanced features like storage, computation, processing, action action-taking capabilities. It also makes decisions based on data obtained from sensors [6]. It manages all application processes based on information obtained from the middleware layer. This application involves sending emails, activating alarms, security system, turning off a device, smartwatch [7].

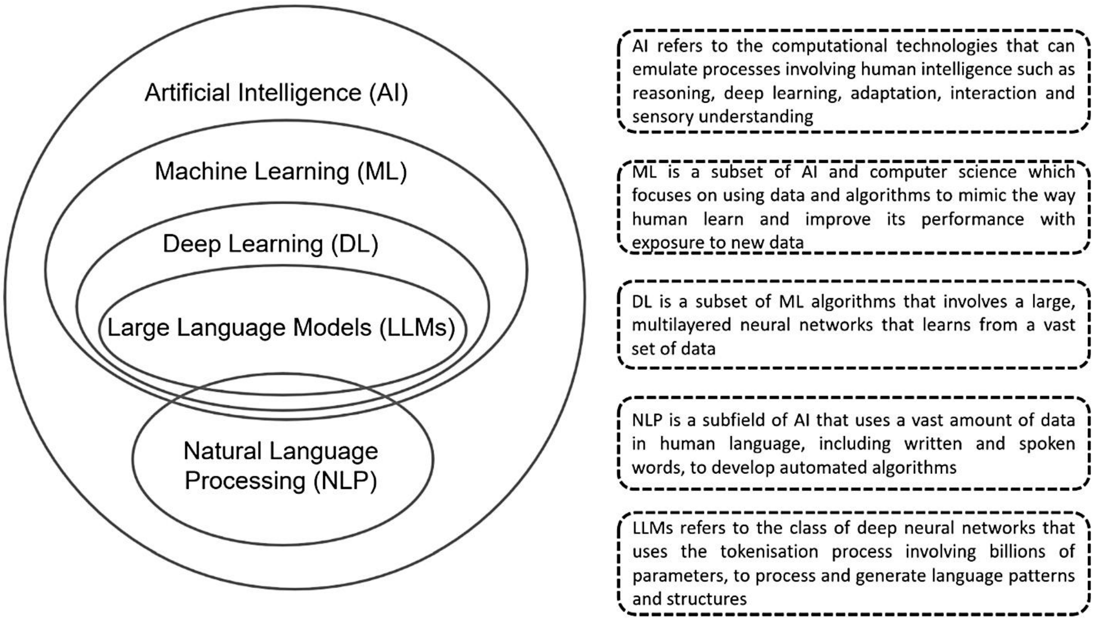
Table 1: GAI's Current Impact [8]



GAI's Impact on Innovation Activities	GAI's Impact on Work Environment	GAI's Impact on Information Infrastructure
Prop. I—Initiators of Innovations: GAI levels the playing field by providing access to expertise, technology, and resources.		
Prop. II—Degree of Innovations: GAI's sweet spot lies in combinations of factual knowledge and creative thinking.	**Prop. IV—People:** GAI has its highest impact on the jobs of white-collar knowledge workers.	
Prop. III—Timing of Innovations: GAI affects most business models initially via value creation innovations.	**Prop. V—Skill Set:** GAI redefines required skill sets as many job roles transform from being creators to becoming editors.	**Prop. VI—Consume or Customize:** "The GAI is out of the bottle." It is not a question if generative AI *will* be used by companies— but *how*.

IoT has the security risk at every architectural layer. In general, the perception layer can suffer from attacks such as malicious code injection, eavesdropping, and interference. Similarly, the network layer is vulnerable to attacks like spoofing, denial of service, man-in-the-middle, and routing information. Privacy is also a major concern which requires a strong authentication system but IoT devices do not have a reliable authentication mechanism because of resource limitations. Finally, the application layer is also open to attack from viruses, worms, and phishing attacks [9, 10].

The integration of AI techniques in IoT systems has a great impact on safeguarding the IoT ecosystem. AI techniques, such as Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) enable IoT systems to analyze vast amounts of data[10] and make intelligent decision making. These techniques also enable the IoT system to detect anomalies and automate security operations against cyberattacks [11].


Artificial Intelligence (AI)
Machine Learning (ML)
Deep Learning (DL)
Large Language Models (LLMs)
Natural Language Processing (NLP)

AI refers to the computational technologies that can emulate processes involving human intelligence such as reasoning, deep learning, adaptation, interaction and sensory understanding

ML is a subset of AI and computer science which focuses on using data and algorithms to mimic the way human learn and improve its performance with exposure to new data

DL is a subset of ML algorithms that involves a large, multilayered neural networks that learns from a vast set of data

NLP is a subfield of AI that uses a vast amount of data in human language, including written and spoken words, to develop automated algorithms

LLMs refers to the class of deep neural networks that uses the tokenisation process involving billions of parameters, to process and generate language patterns and structures

Figure 2: Classification of AI [12]

Generative AI Technology

A robust AI technology in recent years is Generative AI which relies on sophisticated machine learning models that are deep learning (DL) models. The main difference between the deep learning and the machine learning is the structure of the underlying neural network architecture. A traditional machine learning model uses simple neural networks with one or two computational layers. Deep learning models use hundreds or thousands of computational layers to train the models [13]. Generative AI can create original content such as text, images, videos, sound, speech, design art, and simulations in response to a user prompt.

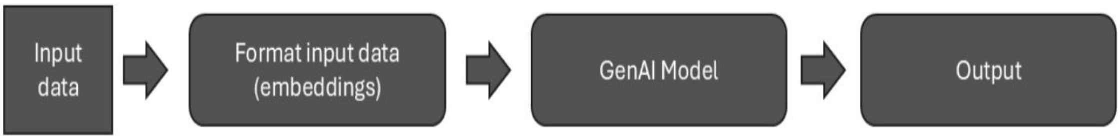


Figure 3: Generative AI General Model [14]

Generative AI Models

Generative AI models are deep learning models that can automatically create content on demand. There are many genAI models, each with unique approaches and applications. Some common models are

Variational Autoencoders (VAEs): A deep learning model includes two connected neural networks. One encodes the huge amount of unstructured data and the other decodes that data parameters to recreate the content. Use for image recognition, natural language processing, and anomaly detection [15].

Generative Adversarial Networks (GANs): Also comprise two neural networks. A generator, which generates new content, and a discriminator which evaluates the accuracy and quality of generated data. It is commonly used for image and video generation.

Transformers: It uses a concept called attention, which means determining and focusing on what is more important in the sequence of data [16].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

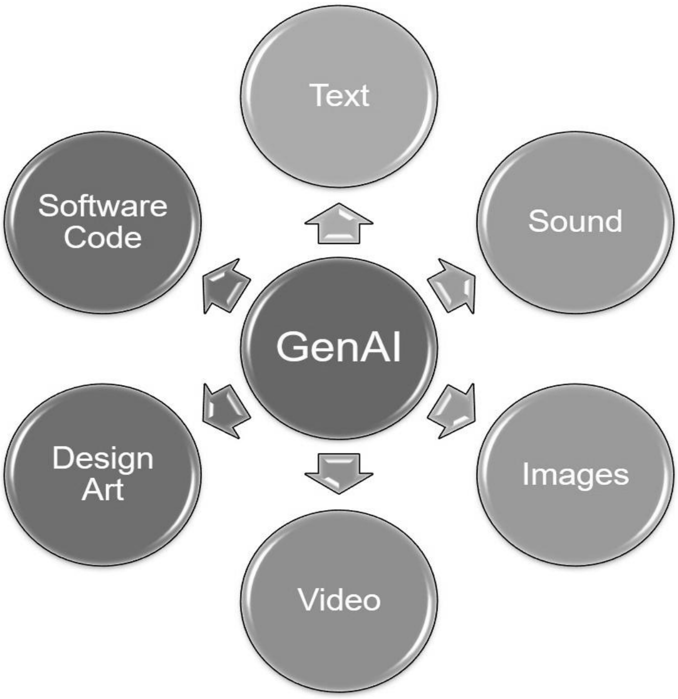


Figure 4: Generative AI Content Creation [17]

IoT systems can improve cyberattack detection, secure communication, and protect data privacy with the help of genAI techniques ultimately creating a robust and reliable IoT ecosystem.

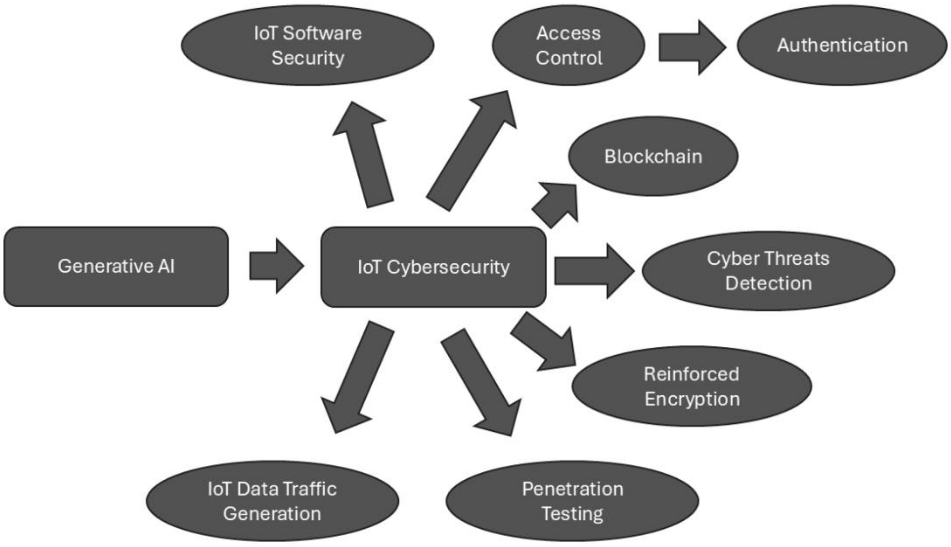


Figure 5: Generative AI in IOT [18]

This survey aims to study the Generative AI techniques that provide the solutions for IoT security challenges. We provide a review of recent research work on Generative AI applications in different areas of IoT security in the entire ecosystem of the IoT environment [19- 21].

The main contributions of this survey are the following:

- It classifies and analyzes the IoT security challenges such as device-level vulnerabilities, network security threats, data security, and privacy concerns.
- It discusses the AI techniques that can improve the security of IoT systems such as cyberattacks and threat detection and prevention algorithms, secure communication, and authentication mechanisms.
- It addresses the privacy challenges associated with IoT data collection and processing.
- It describes the recent study of different genAI models in different areas of IoT cybersecurity [22, 25].

IoT Security Challenges

IoT system security is facing unique challenges that need to be addressed to ensure the integrity, confidentiality, and availability of IoT services. This survey categorizes these challenges in different dimensions [26].

Device-Level Security Challenges:

Device-level security challenges include a range of vulnerabilities and risks associated with individual IoT devices. These challenges must be addressed to ensure the security of IoT systems. The device-level security risks include the following. Physical security is very essential for IoT devices which may include secure enclosures and lock systems to prevent unauthorized access to the devices. It maintains the system's integrity and availability [27, 28]. IoT devices rely on firmware and software components that contain vulnerabilities and malicious actors. Regular patch management is essential to overcome . A strong authentication mechanism such as two-way authentication (2FA) and biometric authentication is essential to prevent unauthorized access to IoT devices. Access control mechanisms such as Role-Based access control (RBAC) and Attribute-Based access control (ABAC) can be implemented to regulate users' access level to prevent the IoT sytem. After addressing these device-level security challenges, organizations can significantly enhance the security of IoT devices [29, 30].

Network & Data Security Challenges

Network security challenges include the deployment of IoT infrastructure that connects IoT devices, and collects and exchange data. The network security risks include the following.

Secure Communication Protocol for IoT Devices: Implementation of secure communication protocols such as Transport Layer Protocol (TLS) and Datagram Transport Layer Protocol (DTLS) is essential for the authenticity of data transmission between IoT devices and backend systems. These protocols employ encryption and digital certificates to establish secure communication channels [31, 32].

Vulnerabilities in Network Infrastructure: the network infrastructure of the IoT system including the routers, gateways and access points can be vulnerable to various cyberattacks. Addressing the network vulnerability is very important to prevent unauthorized access and data breaches [33, 34].

Protection Against Denial of Service attacks. DoS attacks are a big challenge for network security which blocks the network resources for users. The mechanism to detect and mitigate the DoS attacks must be implemented for IoT system availability and reliability.

These network security challenges must be addressed to establish a secure communication infrastructure for IoT system deployments [35, 36]. Data security challenges in IoT systems revolve around the confidentiality, integrity, and privacy of data. Blockchain technology, with its inherent security features such as immutability and decentralization, offers a promising approach to address these challenges by enhancing data security and privacy within the IoT ecosystem. To collect and transmit the sensitive nature of data, robust data security measures are essential. The data security risks include the following.

Data Confidentiality and Encryption Techniques: IoT data often contains sensitive information that has to be prevented from unauthorized access. For this purpose, data encryption techniques such as the Advance Encryption Standard (AES) or Elliptic Curve Cryptography (ECC) are essential to maintain data confidentiality [37, 38].

Data Integrity and Prevention of Tampering: IoT data integrity is important to maintain its accuracy and trustworthiness. For this purpose, digital signature and hash functions help to secure data integrity from unauthorized tampering [39].

Secure Storage and Transmission of IoT Data: Securing storage and transmission of IoT data is very important to prevent unauthorized access. The techniques of Encrypted databases or Hardware Security Modules (HSMs) ensure IoT data storage security and Encrypted communication channels such as HTTPS, and MQTT with TLS establish secure end-to-end communication between IoT devices [40].

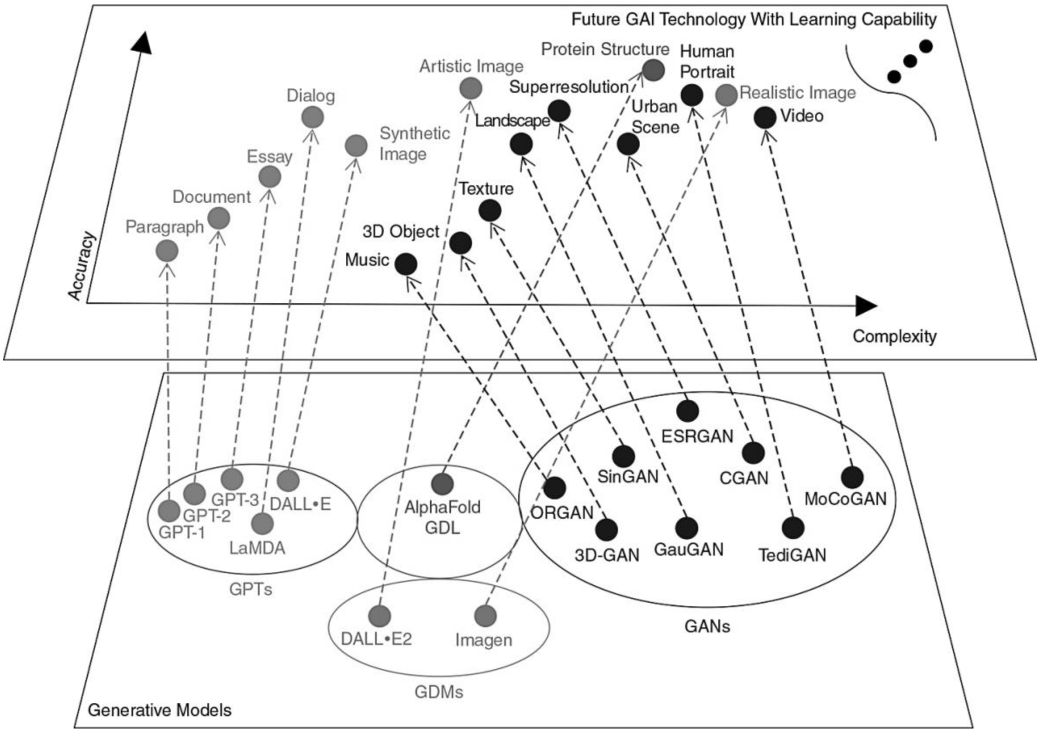


Figure 5: Generative AI models and Artifacts in Data Security [41]

AI Techniques for IoT Security

AI techniques have the potential to significantly enhance the security of IoT systems AI algorithms and models can enable intelligent threat detection and robust authentication mechanisms in IoT systems. Deep learning is a subset of machine learning that is based on multilayer neural networks. These techniques can automatically learn and generate content such as text, images, audio, and videos and can predict the situations according to the pattern and relationships of the specific data set. DL techniques can learn from IoT security data by passing through dataset-trained models such as CNN. The proposed model architecture is fast and accurate. Table 2 represents the summary of deep learning

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

techniques in the IoT environment. Table 2 shows the comprehensive summary of security challenges in IoT systems.

Table 2: IoT Security Challenges

Ref.	Area/Field	Description	Key Measures	Solutions
[42] - [43]	Device-level security challenges.	Measure to secure individual IoT device	Physical security of IoT device Firmware and software vulnerabilities Authentication and access control mechanisms	Secure enclosures, tamper-evident seals, physical locks Regular security assessments, code review, patch management Strong authentication protocols (2FA, biometrics) access control mechanism (RBAC, ABAC)
[44], [45]	Network Security Challenges	Securing communication infrastructure connecting IoT	Secure communication protocols for IoT devices Vulnerabilities	TLS, DTLS Regular assessments, firmware updates, best

Spectrum of Engineering Sciences
Online ISSN
3007-3138
Print ISSN
3007-312X

		devices	in network infrastructure Protection against Denial of service attacks	practices. Monitoring, anomaly detection, rate limitation, traffic filtering
[46] – [47]	Data Security Challenges	Ensuring confidentiality, integrity, and privacy of IoT data	Data confidentiality and encryption techniques Data integrity and prevention of tampering Secure storage and transmission of IoT data	AES, ECC Digital signature, Hash functions Encrypted databases, and secure communication channels (e.g HTTP, MQTT with TLS)
[48] – [49]	Privacy Challenges	Challenges associated with data collection, processing, and user consent in IoT system	Protection of user privacy in IoT data collection and processing Consent management and data ownership Adoption of	Differential privacy, data anonymization Transparent consent mechanisms, and clear data ownership definitions. Secure

	privacy-preserving techniques in IoT system	multiparty computation, and federated learning.

Privacy Challenges

Privacy challenges revolve around user data collection, processing, and user consent. IoT data privacy is very important for user trust. The privacy challenges include the following.

Protection of User Privacy in IoT Data: IoT systems collect vast amounts of data including personal and sensitive information so protecting user privacy is essential. Implementing privacy techniques such as differential privacy and anonymization techniques helps to protect user privacy [50].

Consent Management & Data Ownership: User consent and data ownership is very important. it implements the data privacy mechanism in IoT systems [51].

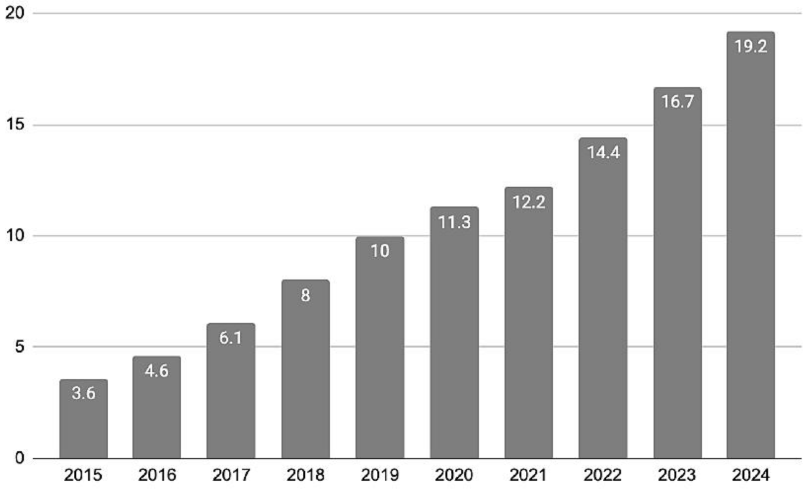


Figure 6: Ratio of IoT connected devices [52]

Adoption of Privacy-Preserving Techniques

In IoT systems, preserving the privacy of sensitive information is an essential part of data seccurity. Techniques such as secure multiparty computation or federated learning allow data analysis without exposing the raw data to a third party [53]. The model shows excellent sensitivity to DoS attacks which are the most dangerous attacks that badly affect the growth of IoT networks. The major benefit of DL over conventional machine learning is its higher level and accuracy on massive datasets. DL techniques can be used in IoT security to improve anomaly detection and malicious activities as well as to protect the privacy of IoT device users. Modern AI techniques, including DL, transformers, and GenAI have a vital role in enhancing IoT security against advanced cyber threats in fast-changing IoT systems.

Table 3: DL Techniques in IoT Security

Ref.	AI Approach	Security Objective	Dataset	Accuracy
[53]	CNN	Malware Detection	IoTPoT	95%
[54]	CNN	Medical Image Security	MRI Dataset	-
[54]	CNN	Malware Detection	IoT_Malware dataset	97.93%
[55]	CNN	Malicious data identification	Kitsune network attack database	95.93%
[56]	RNN	Intrusion detection	NSL-KDD	97.35%
[57]	RNN	Intrusion detection	DARPA/KDD Cup '99	98.91%
[57]	DNN	Anomaly detection	IoT-Botnet 2020	99%

[58]	MLP	Botnet attack detection	Captured from 9 IoT devices	99%

Deep learning is ideal for intrusion protection and anomaly detection because of its processing power and ability to recognize complicated patterns in big datasets. For example, network security systems use DL algorithms to spot suspicious patterns that might be signs of an attack. IoT Cybersecurity is making more use of GenAI model transformers, which are well-known for their efficiency in processing sequential data. With the help of these techniques, we can protect ourselves against security breaches by analyzing time-series data from IoT devices. Likewise, there are significant consequences for cybersecurity in the IoT from GenAI like ChatGPT. It helps create security model training data, sophisticated protection techniques, and simulating cyberattacks. This technology is quickly becoming a critical component of advanced IoT cybersecurity.

Conclusion

As countries around the world are working toward regulating AI-based health systems using the total product lifecycle and high-risk approaches, it is essential to address the regulatory gaps. This paper offers a comprehensive systematic literature review of recent advancements in the field of generative AI. Specifically, it thoroughly explores key algorithms within the realm of Generative AI Every domain uses IoT devices to collect real-time data and analyze that data for decision-making to improve processes. Therefore, Securing IoT infrastructure is essential for upcoming growth and advancement in this system. Instead of traditional security measures, AI techniques are more effective in enhancing the overall security of IoT systems.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Cellular IoT Connections Reached 3.4 Billion in 2023. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

[2] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[3] Imtiaz, Ahsan, Danish Shehzad, Fawad Nasim, Muhammad Afzaal, Muhammad Rehman, and Ali Imran. "Analysis of Cybersecurity Measures for Detection, Prevention, and Misbehaviour of Social Systems." In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 1-7. IEEE, 2023.

[4] Hassan, Salman, Danish Irfan, Fawad Nasim, Polycarp Shizawaliyi Yakoi, Muhammad Mansab, and Saleem Zubair. "Room Occupancy Detection Using IoT Sensor Data and Machine Learning." International Journal of Social Science Archives (IJSSA) 7, no. 3 (2024).

[5] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity

and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[6] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, ''The security of big data in fog-enabled IoT applications including blockchain: A survey,'' Sensors, vol. 19, no. 8, p. 1788, Apr. 2019.

[7] Nasim, Fawad, Sohail Masood, Arfan Jaffar, Usman Ahmad, and Muhammad Rashid. "Intelligent Sound-Based Early Fault Detection System for Vehicles." Computer Systems Science & Engineering 46, no. 3 (2023).

[8] Cellular IoT Connections Reached 3.4 Billion in 2023. Available online: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/iot-connections-outlook

[9] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

[10] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[11] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[12] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional

Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[13] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[14] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[15] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[16] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[17] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[18] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[19] Abdullah, M., Khan, H., Shafqat, A., Daniyal, M., Bilal, M., & Anas, M. (2024). Internet of Things (IoT's) in Agriculture:

Unexplored Opportunities in Cross–Platform. Spectrum of engineering sciences, 2(4), 57-84.

[20] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[21] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[22] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[23] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

[24] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[25] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[26] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of

Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[27] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[28] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[29] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[30] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[31] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[32] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, “An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[33] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[34] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[35] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[36] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[37] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[38] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[39] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In

2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[40] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[41] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[42] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[43] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[44] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[45] Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced

persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.

[46] Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.

[47] Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

[48] Mutalib, Noor Hazlina Abdul, et al. "Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: a review." Artificial Intelligence Review 57.11 (2024): 1-47.

[49] Yang, Lu-Xing, et al. "Defense against advanced persistent threat through data backup and recovery." IEEE Transactions on Network Science and Engineering 8.3 (2020): 2001-2013.

[50] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system", Proc. Int. Symp. Consum. Electron. (ISCE), pp. 1-2, Jun. 2015.

[51] H. N. Rafsanjani and A. Ghahramani, "Towards utilizing Internet of Things (IoT) devices for understanding individual occupants' energy usage of personal and shared appliances in office buildings", J. Building Eng., vol. 27, Jan. 2020.

[52] F. Loukil, C. Ghedira-Guegan, A. N. Benharkat, K. Boukadi and Z. Maamar, "Privacy-aware in the IoT applications: A systematic literature review", Proc. On Move Meaningful Internet Syst. Conf. (OTM), pp. 552-569, 2017.

[53] S. Aheleroff, X. Xu, Y. Lu, M. Aristizabal, J. P. Velásquez, B. Joa, et al., "IoT-enabled smart appliances under industry 4.0: A case study", Adv. Eng. Informat., vol. 43, Jan. 2020

[54] P. J. Basford, F. M. J. Bulot, M. Apetroaie-Cristea, S. J. Cox and S. J. Ossont, "LoRaWAN for smart city IoT deployments: A long term evaluation", Sensors, vol. 20, no. 3, pp. 648, Jan. 2020

[55] E. Symeonaki, K. Arvanitis and D. Piromalis, "A context-aware middleware cloud approach for integrating precision farming facilities into the IoT toward agriculture 4.0", Appl. Sci., vol. 10, no. 3, pp. 813, Jan. 2020

[56] M. S. Kaiser, K. T. Lwin, M. Mahmud, D. Hajializadeh, T. Chaipimonplin, A. Sarhan, et al., "Advances in crowd analysis for urban applications through urban event detection", IEEE Trans. Intell. Transp. Syst., vol. 19, no. 10, pp. 3092-3112, Oct. 2018.

[57] S. Selvaraj and S. Sundaravaradhan, "Challenges and opportunities in IoT healthcare systems: A systematic review", Social Netw. Appl. Sci., vol. 2, no. 1, pp. 139, Dec. 2019.

[58] M. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem and H. Basiron, "A review on security challenges and features in wireless sensor networks: IoT perspective", J. Telecommun. Electron. Comput. Eng., vol. 10, no. 1, pp. 17-21, Feb. 2018.